Bachelorarbeit

IPv6 Sicherheit im LAN: Bedrohungen und Maßnahmen

André Domnick

26. Februar 2014

Version 1.01

Hochschule Offenburg
Fakultät M+I
Unternehmens- und IT-Sicherheit

Bearbeitungszeitraum

01. 11. 2013 – 28. 02. 2014

Betreuer Hochschule Offenburg:

Prof. Dr. rer. nat. Daniel Hammer

Betreuer Unternehmen:

Dr. Safuat Hamdy

Secorvo Security Consulting GmbH

Erklärung

Hiermit erkläre ich, dass ich diese Abschlussarbeit selbständig verfasst habe, keine anderen als die angegebenen Quellen/Hilfsmittel verwendet habe und alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten Schriften entnommen wurden, als solche kenntlich gemacht habe. Darüber hinaus erkläre ich, dass diese Abschlussarbeit nicht, auch nicht auszugsweise, bereits für eine andere Prüfung angefertigt wurde.

André Domnick, 26. Februar 2014

Zusammenfassung

In dieser Arbeit werden die Bedrohungen für ein lokales IPv6 Netzwerk, mit besonderem Hinblick auf das neu eingeführte Neighbor Discovery Protocol (NDP), analysiert. Dabei wird der Frage nachgegangen, wie ein IPv6 Netz gegen lokale Angriffe geschützt werden kann. Zunächst werden mögliche Angriffe auf das Netzwerk beschrieben. Gegen die dann jeweils Maßnahmen vorgestellt werden. Die Funktionsweise der Maßnahmen wird erläutert und die mit Einführung sowie Betrieb verbundenen Kosten und Nutzen eingeordnet. Darauf basierend wird eine Bewertung der Maßnahmen durchgeführt, um konkrete Handlungsempfehlungen zum sicheren Betrieb von IPv6 Netzen in der Praxis zu geben. In der Bewertung wird deutlich, dass ein Großteil der Maßnahmen noch nicht ausgereift oder nur bedingt praktisch anwendbar erscheint. Reaktive Maßnahmen wie NDPMon eignen sich dabei nach Ergebnissen der Analyse am besten zur Absicherung von NDP Verkehr. Um die Integration von NDPMon durch eine einheitliche Plattform zu erleichern, wird ein Einsatzbeispiel auf Basis des ARM-Einplatinencomputer Raspberry Pi beschrieben. Abgeschlossen wird die Arbeit mit einem Fazit zur lokalen Absicherung von IPv6 Netzwerken und den damit verbundenen Herausforderungen, sowie einem kurzen Ausblick auf zukünftige Entwicklungen im Bezug auf Schutzmaßnahmen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Das Internet Protokoll (IP) ermöglicht im Internet erst die Kommunikation zwischen zwei Systemen, die sich nicht im gleichen lokalen Netz befinden. Es bildest dabei die Umsetzung der Vermittlungsschicht, also der Schicht 3 nach OSI Modell [ITUX200, S. 28]. Die Sicherungsschicht (Schicht 2 im OSI Modell) ermöglicht es lediglich im gleichen lokalen Netz befindlichen Systemen miteinander zu kommunizieren. Während die Vermittlungsschicht für die globale Adressierbarkeit der Systeme sowie die Wegfindung im Internet sorgt. Um ihr Ziel zu erreichen, werden die Pakete bei IP über einen Pfad von Knoten zum Ziel weitergeleitet. Diese Knoten werden als Router bezeichnet. Aktuell wird das IP Protokoll in der Version 4 eingesetzt, kurz IPv4. Die Anzahl, der mittels IPv4 adressierbaren Adressen ist auf 2^{32} beschränkt. Ein Großteil dieser Adressen wurde bereits von den Registraren vergeben.[1] Daher kommt es zu einer wachsenden Adressknappheit.[2]

Als Nachfolger für IPv4 wurde schon 1998 das IP in der Version 6, also IPv6, durch die Internet Engineering Task Force (IETF) standardisiert. IPv6 konnte sich jedoch bisher nicht in der Praxis verbreiten und fristete somit bisher eher ein Nischendasein. In Folge der Adressknappheit gibt es jedoch in den letzten Jahren einen andauernden Anstieg der praktischen Nutzung von IPv6.[3] Mittlerweile bieten Internet Service Provider (ISPs) wie Telekom, Kabel Deutschland, Kabel BW teilweise auch den Endkunden native IPv6-Unterstützung an. Neukunden von Unitymedia, wozu auch Kabel BW gehört, erhalten seit 2013 sogar nurnoch IPv6 Adressen auf ihren Internetzugangsleitungen.[4] Weiter unterstützt wird dieser Trend dadurch, dass beispielsweise unter Windows 7 IPv6 standardmäßig aktiviert ist. In Folge dessen

[1] http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8 - Abruf am 19.01.2014

[2] http://www.potaroo.net/tools/ipv4/index.html - Abruf am 19.01.2014

[3] http://www.enterprisenetworkingplanet.com/netsp/ipv6-launch-day-one-year-later.html - Abruf am 19.01.2014

[4] http://www.onlinekosten.de/news/artikel/51398/0/Unitymedia-Neukunden-erhalten-nur-noch-IPv6-Adressen - Abruf am 05.02.2014

müssen sich auch immer mehr Unternehmen mit IPv6 in ihren Netzen beschäftigen, auch wenn sie aktiv noch keine Verwendung von IPv6 in ihren Netzen planen. Andernfalls könnten über IPv6, Angriffe an den bestehenden Netzwerksicherheitsmaßnahmen vorbei, durchgeführt werden. Durch die tiefgreifenden Protokolländerungen ist IPv6 für einige der relevanten Angriffe von IPv4 nicht mehr verwundbar. Jedoch bringen die neu eingeführten Funktionen, wie z.B. die Neighbor Discovery, neue Angriffsvektoren mit sich. Reichte es früher aus das Netzwerk vor Angriffen über IPv4 abzusichern, so kommt beim Dual-Stack-Betrieb die Absicherung gegen Bedrohungen über IPv6 hinzu. Soll nur IPv4 genutzt werden, so sollte IPv6 zumindest deaktiviert und IPv6 Verkehr durch die Firewalls blockiert werden.

Diese Arbeit beschäftigt sich mit den Bedrohungen gegen IPv6 in einem LAN und verschiedenen Schutzmaßnahmen. Es existiert schon zahlreiche Schutzmaßnahmen, die Angriffe gegen IPv6 verhindern sollen. Diese Maßnahmen versuchen die Probleme auf verschiedenen Ebenen zu lösen, beispielsweise durch Erweiterung der Funktionen von Netzwerkhardware oder durch kryptografische Verfahren. Jedoch bleibt dabei offen, welche der Maßnahmen in der Praxis zur Verhinderung der Angriffe überhaupt geeignet und empfehlenswert sind. Deshalb sollen die Maßnahmen betrachtet und jeweils die mit ihnen verbundenen Kosten und Nutzen analysiert werden. Basierend darauf werden die Maßnahmen bewertet und konkrete Einsatzempfehlungen gegeben.

Der offensichtlichste Unterschied zwischen IPv4 und IPv6 ist die Größe des Adressraums. IPv6 unterscheidet sich von IPv4 jedoch durch weit mehr als den mit von 128 statt 32 Bit um Größenordnungen größeren Adressraum. Daher ist es zum Verständnis der Bedrohungen und deren Abwehr notwendig, zuerst die Protokolländerungen zu verstehen. Da eine komplette Protokollerläuterung und Einführung in IPv6 das Maß der Arbeit alleine sprengen könnte und es schon entsprechende Einführungen gibt, sei für eine kurze Einführung in IPv6 auf Kapitel 2 des IPv6 Secorvo Whitepapers von Safuat Hamdy [HDYv6WP] sowie auf das Buch „IPv6. Grundlagen - Funktionalität - Integration“ von Silvia Hagen [IPv6HAGEN09] verwiesen. Eine Kenntnis der Protokollgrundlagen wird im Folgenden vorausgesetzt.

Die mit IPv6 verbundenen Neuerungen bedingen auch eine teilweise neue Terminologie. Die wichtigsten Begrifflichkeiten werden nachfolgend kurz eingeführt. Siehe auch das Glossar am Ende dieser Arbeit.

1.1. Terminologie

Bei IPv6 werden Datenpakete zwischen Systemen ausgetauscht. Die dabei versendeten Pakete bestehen aus einem IP-Header, welcher die protokollspezifischen Informationen, wie Quell- und Zieladresse, enthält und aus einer Payload. Die Payload beinhaltet die Nutzdaten der nächst höheren Protokollschichten, man spricht von den Upper Layer Protocols (ULP). Bei den ULPs für IP handelt es sich in der Regel um ICMP, TCP oder UDP.

Ist ein System über eine Netzwerkschnittstelle (Interface) mit einem Netzwerk verbunden, so wird es nachfolgend als Node bezeichnet. Ein Router ist eine spezielle Form eines Nodes, der IP Pakete auf einem oder mehreren Interfaces annimmt und anhand seiner Routingtabelle weiterleitet. Nodes bei denen es sich nicht um Router handelt, sondern nur um normale angeschlossene Systeme, werden nachfolgend als Endsysteme bzw. Endgeräte bezeichnet.

Ein Link bezeichnet das Netzwerk aller Nodes, die direkt, ohne einen Router, miteinander kommunizieren können. Befindet sich das Zielsystem auf dem gleichen Link, so wird es als on-link bezeichnet. IPv6 führt die Bezeichnung von Systemen, die sich auf dem gleichen Link befinden, als Nachbarn ein, man spricht von Neighbors. Diese Bezeichnung findet sich auch beispielsweise im Neighbor Discovery Protocol (NDP) wieder. Zielsysteme, die sich nicht auf dem gleichen Link befinden, mit denen also über mindestens einen Router kommuniziert werden muss, werden als off-link bezeichnet.

Eine Verbindung in das restliche Internet, in der Regel mittels eines ISPs, wird nachfolgend als Uplink bezeichnet. Einer solchen Verbindung werden ein oder mehrere Präfixe zugeordnet, die eine globale Kommunikation erlauben. Diese Präfixe bilden für die über den Uplink angebundenen Geräte die Grundlage zur Bildung globaler IPv6 Adressen.

Der Begriff Performance, im Bezug auf ein Netzwerk, beschreibt nachfolgend die Leistungsfähigkeit des Netzes. Diese zeichnet sich insbesondere durch verfügbare Bandbreite bzw. Datenrate, die Antwortzeiten und die Zuverlässigkeit des Netzes aus.[5]

[5] Orientierung an Bewertungskriterien der Performance-Architektur nach [Boek2012, Kap 5.4]

2. Problemdefinition

In diesem Kapitel sollen die Grundlagen der Bedrohungsanalyse des IPv6 Netzwerkprotokolls im LAN definiert werden. Zuerst wird dafür das betrachtete Thema abgegrenzt. Darauf basierend werden die Sicherheitsziele spezifiziert, die gewährleistet werden sollten. Anschließend wird bestimmt, welche möglichen Angreifer betrachtet werden und mit welchen Fähigkeiten diese ausgestattet sind. Für diese Angreiferrollen werden dann verschiedene Angriffstypen beschrieben, die die Schutzziele des Netzwerks bedrohen.

2.1. Abgrenzung des Analyseobjekts

Im Fokus der hier durchgeführten Analyse sind lokale Netzwerke, die IPv6 als Vermittlungsschicht (Schicht 3 im OSI Modell [ITUX200, S.28]) einsetzen. Dabei kann entweder nur IPv6 oder sowohl IPv6 als auch IPv4 eingesetzt werden. Bei Letzterem spricht man vom Dual-Stack Betrieb. Dabei beschränkt sich die Untersuchung ausschließlich auf die IPv6-spezifischen Bedrohungen.

Zudem sollen nur die Bedrohungen beachtet werden die auf dem Link, also in dem lokalen Netzwerk (LAN), existieren. Die Sicherstellung der Perimetersicherheit, also die Absicherung des Netzwerks nach außen, beispielsweise durch Firewalls, wird hier nicht weiter untersucht. Zu diesem Thema existiert bereits Literatur, wie beispielsweise das Buch [CiscoIPv6Sec] von Cisco Press, welches die Maßnahmen zur Absicherung der Perimeters genau beschreibt.

Als Anwendungsmodell wird von dem Netzwerk eines Unternehmens ausgegangen, in dem sich im Normalfall alle Systeme unter der administrativen Kontrolle der Systemadministratoren befinden. Ausnahmen wie das immer beliebter werdende *Bring you own device*, bei dem Mitarbeiter eigene Geräte im internen Netz verwerden, werden hier nicht betrachtet.

Ein Angreifer bedroht die Sicherheit des internen Netzes, indem er versucht es abzuhören, teilweise unter seine Kontrolle zu bringen oder die Verfügbarkeit des Netzes negativ zu beeinflussen.

Bei der Analyse wird dort, wo es zur Erläuterung von Risiken und Maßnahmen notwendig ist, auf die Sicherheitsfunktionen sowie Eigenschaften der niedrigeren und höheren Protokollschichten des OSI Modells eingegangen. Der Schwerpunkt liegt dabei aber explizit auf den, mit der Neueinführung von IPv6 verbundenen Änderungen und ihren Folgen für die Netzwerksicherheit. Der Kernbestandteil dessen ist die Absicherung des Neighbor Discovery Protocol (NDP) [RFC4861].

2.2. Schutzziele

Um festzustellen welche Bedrohungen für ein Netzwerk existieren, sollten zuerst die Schutzziele definiert werden, die für das Netz gewährleistet sein müssen, um eine sichere Kommunikation zu ermöglichen. Hierbei gibt es in der Informationssicherheit eine Reihe grundlegender Ziele, die verschieden granular gestaltet sein können. Diese Analyse beschränkt sich dabei auf die drei Kernziele (nach [ISecFund04, S. 18ff.][Schaefer2003, S. 8, S. 15f]) Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability), die wegen der ersten Buchstaben der englischen Namen auch als C-I-A-Ziele bezeichnet werden.

2.2.1. Vertraulichkeit

Vertraulichkeit bedeutet, dass lediglich die dazu autorisierten Personen in der Lage sein dürfen, die übertragenen oder gespeicherten Daten zu lesen. Im Fokus der Netzwerksicherheit steht ausschließlich die Übertragung. Dies bedeutet, dass es keinem Angreifer möglich sein darf die übertragenen Daten auszulesen.

Zum Schutz der Vertraulichkeit wird im Bereich der Netzwerksicherheit üblicherweise die Kommunikation verschlüsselt. Ein Angreifer kann so aus mitgehörtem Netzwerkverkehr nicht die Inhalte rekonstruieren.

2.2.2. Integrität

Integrität bedeutet, dass nur dazu autorisierte Personen Daten verändern dürfen. Die Daten also geeignet vor der Manipulation durch unbefugte Dritte geschützt sein müssen. Oft wird unter Integrität auch zusätzlich verstanden, dass getätigte Änderungen nachvollziehbar sind und sicher einer Person zugeordnet werden können.

Im Bezug auf die Sicherheit von Kommunikation beschreibt Integrität, dass kein Dritter manipulativ auf die Kommunikation zwischen zwei Systemen einwirken darf. Der Verkehr darf also beispielsweise nicht durch einen Angreifer verändert werden können. Ist eine Veränderung durch einen Angreifer möglich, so muss diese den Kommunikationsparteien als Integritätsverletzung kenntlich gemacht werden.

2.2.3. Verfügbarkeit

Verfügbarkeit bedeutet, dass die Daten oder Dienste, möglichst immer für die dazu autorisierten Personen nutzbar sind. Dies umfasst sowohl die Sicherstellung, dass möglichst keine Ausfälle auftreten, als auch die Gewährleistung der Performance des Zugriffs.

Die Verfügbarkeit stellt insofern ein elementares Schutzziel dar, als ein Dienst oder Netzwerk welches nicht oder nicht zuverlässig genutzt werden kann seinen Zweck nicht erfüllt.

2.3. Angreifer

Die hier betrachteten Bedrohungen der Netzwerksicherheit, werden durch bewusstes Einwirken einer Person auf das Netz herbeigeführt. Als Angreifer wird nachfolgend eine Person bezeichnet, die versucht das Netzwerk anzugreifen und zu manipulieren.

Dabei werden zwei Kategorien von Angreifern unterschieden, der interne und der externe Angreifer. Sie besitzen verschiedene Möglichkeiten die Schutzziele des Netzwerks durch Angriffe zu bedrohen.

2.3.1. Interner Angreifer

Der interne Angreifer oder Innentäter, ist eine Person, die rechtmäßiger Teil der Netzwerkes ist, bzw. rechtmäßigerweise Zugang zu den Systemen besitzt. Ein Beispiel eines internen Angreifers könnte beispielsweise ein frustrierter oder gekündigter Mitarbeiter sein, der dem Unternehmen Schaden zufügen oder sich selbst bereichern möchte.

Durch seine Position verfügt der interne Angreifer bereits über Zugang zu Endgeräten und somit auch zum Netzwerk. Möglicherweise verfügt er ebenfalls über (phyikalischen) Zugang zu Teilen der Netzwerkinfrastruktur.

So kann der Angreifer direkt, mittels manipulierter Pakete, Einfluss auf das Netzwerk nehmen und muss dabei in vielen Fällen keine weiteren Schutzmaßnahmen überwinden. Besonders wegen des oft weitreichenden Zugriffs und der fehlenden Schutzmaßnahmen geht von dieser Art des Angreifers in vielen Fällen eine große Gefahr aus.

Dadurch, dass der Zugang zum Netz grundlegend legitimiert ist, können dauerhafte oder wiederkehrende Angriffe ohne großes Aufsehen durchgeführt werden. So wird das Schadenspotential weiter erhöht.

2.3.2. Externer Angreifer

Der externe Angreifer besitzt keinen rechtmäßigen Zugriff auf das lokale Netzwerk. Es könnte sich beispielsweise um einen Konkurrenten mit Absicht der Industriespionage oder Sabotage handeln.

Um in dem internen Netzwerk operieren zu können, müssen hier zuerst die Perimetersicherheitsmaßnahmen überwunden werden. Dazu kann versucht werden interne Endgeräte, beispielsweise mittels Phishing, zu kompromittieren und so eine Möglichkeit zum Zugriff auf das interne Netz zu erhalten.

Alternativ wird direkt von außen versucht die Perimeterschutzmaßnahmen zu überwinden und so in das Netzwerk einzudringen. Ist das erste System im internen Netz unter der Kontrolle des Angreifers, kann er dieses dazu nutzen um weitere Angriffe auf das LAN durchzuführen.

Externe Angriffe können durch die Umsetzung einer guten Perimetersicherheit wesentlich erschwert werden. Außerdem erregen sie, im Gegensatz zu internen Angrif-

fen, eher Aufmerksamkeit, da eine Kommunikation zum Angreifer über die Perimetergrenze hinweg erfolgen muss. Oft werden beispielsweise Network Intrusion Detection Systeme (NIDS) eingesetzt, die zumindest einen Teil solcher Angriffe erkennen können.

Im Folgenden wird angenommen, dass es dem Angreifer gelungen ist direkten Zugriff zum Link zu erlangen. Es ist ihm so möglich Datenpakete seiner Wahl zu versenden. Unter dieser Voraussetzung kann der externe Angreifer das interne Netzwerk auf die gleichen Arten angreifen wie der Interne.

2.4. Angriffstypen

Grundsätzlich können bei Angriffen auf ein LAN mehrere verschiedene Angriffsarten unterschieden werden. Jede von ihnen richtet sich gegen eines oder mehrere der in Abschnitt 2.2 definierten Schutzziele. Die verschiedenen Arten der Angriffe orientieren sich jeweils an denen die Fernando Gont in [GONTND13, S. 39] unterscheidet:

2.4.1. Denial of Service Angriff

Ein Denial of Service (DOS) Angriff richtet sich gegen die Verfügbarkeit des Netzes oder Teile dessen. Dabei wird versucht die legitime Kommunikation zu unterbinden.

Dies kann beispielsweise dadurch geschehen, dass der Netzwerkverkehr durch modifizierte Adressauflösungen ins Nichts geleitet wird. Alternativ könnte verhindert werden, dass ein System am LAN überhaupt teilnehmen kann, indem es daran gehindert wird sich eine Adresse zuzuweisen bzw. zugewiesen zu bekommen.

2.4.2. Performance Degrading

Ein Performance Degrading Angriff richtet sich ebenfalls gegen die Verfügbarkeit des Netzes. Jedoch wird hier nicht beabsichtigt die Kommunikation gänzlich zu unterbinden, sondern lediglich die Performance des Netzes so zu manipulieren, dass dessen Verwendung negativ beeinflusst wird.

Unter Umständen, beispielsweise bei zeitkritischen Anwendungen oder wenn eine Software auf eine Antwort in einem bestimmten Zeitraum angewiesen ist, kann

durch die Reduktion der Performance auch gleichzeitig die Funktionsfähigkeit eingeschränkt werden. Ein Performance Degrading Angriff kann unter solchen Voraussetzungen auch zu einen Denial of Service führen.

2.4.3. Traffic Hijacking

Der Traffic-Hijacking- oder auch Man-in-the-Middle-Angriff beschreibt einen Angriff, sowohl auf die Integrität als auch auf die Vertraulichkeit der zu schützenden Daten.

Dabei leitet ein Angreifer den Netzwerkverkehr zwischen dem Opfer und einem Ziel, mit dem das Opfer kommuniziert, über ein vom Angreifer kontrolliertes System um. An diesem System kann der Verkehr mitgehört und so dessen Vertraulichkeit verletzt werden. Außerdem kann der Angreifer aktiv Modifikationen an dem umgeleiteten Netzwerkstrom durchführen, sodass eine Integritätsverletzung stattfindet.

Durch das Verwerfen von Netzwerkverkehr kann auch die Verfügbarkeit angegriffen und so ein Denial of Service erzeugt werden. Bei einem derartigen Angriff spricht man vom sogenannten *Blackholing*.

Mit einem Traffic Hijacking Angriff können alle drei Schutzziele verletzt werden. Aufgrund dessen ist ein so gearteter Angriff, im Vergleich zu den anderen Angriffstypen, mit dem höchsten Schadenpotential verbunden.

3. Angriffe gegen das Neighbor Discovery Protocol

In diesem Abschnitt werden praktische Angriffe auf das IPv6 Neighbor Discovery Protocol vorgestellt, um die Bedrohungen zu konkretisieren. Diese Angriffe werden dabei jeweils den in Abschnitt 2.4 vorgestellten Angriffstypen zugeordnet.

Mit IPv6 wurde das Neighbor Discovery Protocol (NDP) [RFC4861] neu eingeführt. Es ersetzt die Funktion des ARP Protokolls [RFC826] aus IPv4 und übernimmt weitere wichtige Verwaltungsaufgaben in einem IPv6 Netzwerk. Da das Protokoll nicht explizit mit dem Ziel der Resistenz gegenüber Angriffen entworfen wurde, bietet es wegen seiner elementaren Rolle in jeder IPv6 Umgebung einen ausgezeichneten Vektor für Angriffe auf die Sicherheit des Netzes.

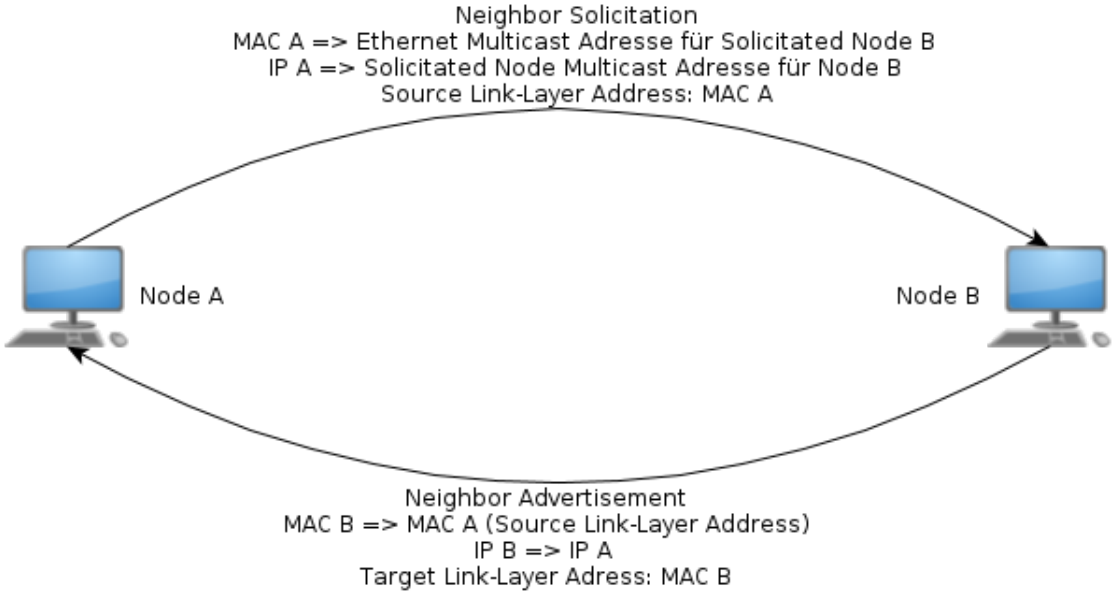
Die Adresszuweisung in IPv6 Netzen erfolgt meistens mittels dezentraler Adresszuweisung, der Stateless Address Autoconfiguration (SLAAC). Wenn eine IPv6 Adresse zugewiesen werden soll, verwenden die Nodes die Duplicate Address Detection (DAD), um herauszufinden ob die Adresse bereits vergeben ist. Die Duplicate Adress Detection ist wiederum Teil von NDP.

NDP ermöglicht es Routern sogenannte Router Advertisements (RA) zu versenden. So kann den Nodes mitgeteilt werden, durch welchen Router welche Routen bedient werden und welche Präfixe dabei zur Verfügung stehen.

3.1. Neighbor Discovery

Die in [RFC4861, Kap 7] beschriebenen Neighbor Advertisement und Neighbor Solicitation Nachrichten ersetzen in IPv6 Netzen das ARP Protokoll. Sie bieten die Möglichkeit der Auflösung von IPv6 Adressen zu Adressen der Schicht 2 (z.B. MAC). So wird es möglich Nachrichten direkt an andere Nodes des gleichen Links zu senden.

Mittels einer Neighbor Solicitation bittet ein Node über Multicast den Inhaber der gesuchten IPv6 Adresse um dessen Schicht 2 (z.B. MAC) Adresse. Wird die IPv6 Adresse gerade von einem Node verwendet, so antwortet dieser mit einem Neighbor Advertisement, das die angeforderte Schicht 2 Adresse enthält. Der Anfrager kann so eine Assoziation zwischen Adressen der Schicht 3 (IPv6) und der Schicht 2 (z.B MAC) hergestellen.



Node A ermittelt die zu Node B gehörende Schicht 2 Adresse mittels Neighbor Discovery

Abbildung 3.1.: Funktionsweise Neighbor Solicitation und Advertisement

Wird von einem Node eine Neighbor Advertisement empfangen, so wird die damit hergestellte Assoziation für die zukünftige Verwendung im Neighbor Cache gespeichert.

Die Speicherung im Neighbor Cache sollte nur geschehen, wenn das Neighbor Advertisement durch eine Neighbor Solicitation von dem betreffenen Node angestoßen wurde. Andernfalls muss nicht davon ausgegangen werden, dass mit der entsprechenden Entität kommuniziert werden soll. Dieses Vorgehen wird aber in [RFC4861, Kap 7] nur empfohlen und nicht erzwungen, sodass unter Umständen auch Systeme bei Empfang eines Neighbor Advertisements einen Neighbor Cache Eintrag erstellen, ohne zuvor eine Neighbor Solicitation dafür gesendet zu haben.

Dies könnte beispielsweise damit begründet werden, dass die Performance erhöht

wird, da die Assoziation für eventuelle zukünftige Kommunikation schon vorhanden ist.

Wenn ein Node eine Neighbor Solicitation empfängt die Quelladressen für Schicht 2 und 3 enthält, wird ebenfalls ein Neighbor Cache Eintrag erstellt. Da die Kommunikation immer bidirektional stattfindet, kann so eine zweite Neighbor Discovery für die Antwortrichtung eingespart werden.

Traffic Hijacking Angriff

Eine Authentisierung des Absenders von Neighbor Advertisements oder Solicitations ist nicht vorgesehen. Der Absender muss also nicht beweisen, dass er wirklich der Inhaber der entsprechenden IPv6 Quelladresse ist.

Somit ist es einem Angreifer möglich, beliebige Neighbor Discovery Nachrichten zu versenden und dadurch falsche Assoziationen bei den anderen Nodes des Links zu erzeugen. Durch die neuen Nachrichten können sogar alte Einträge im Neighbor Cache überschrieben werden. Dabei wird davon ausgegangen, dass sich die Schicht 2 Adresse geändert haben könnte. Dementsprechend wird immer die Information des aktuellsten Neighbor Advertisements verwendet, um die Aktualität der Neighbor Cache Einträge zu gewährleisten.

Ein Angreifer kann, wie in [RFC3756, Kap 4] beschrieben, den Netzwerkverkehr zwischen zwei auf dem gleichen Link befindlichen Nodes über sein System umleiten. Dazu verwendet er jeweils auf die Schicht 2 Adresse eines unter seiner Kontrolle befindlichen Systems verweisende Neighbor Cache Einträge. Durch eine derartige Umleitung befindet er sich als Man-in-the-Middle zwischen den Systemen und kann den Netzwerkverkehr mithören oder verändern. Dieser Angriff ist das IPv6-Äquivalent des ARP-Spoofing Angriffs auf IPv4, man spricht hier von Neighbor Cache Poisoning.

Es handelt sich bei Neighbor Cache Poisoning um einen Traffic Hijacking Angriff, wie er in 2.4.3 beschrieben wurde. Der Angriff kann durch einen Angreifer der Zugriff auf den Link hat, sehr einfach durchgeführt werden und hat schwerwiegende Auswirkungen auf die Sicherheit des Netzes.

In Abb. 3.2 wird der Ablauf eines Neighbor Cache Poisoning Angriffs beschrieben. In dem Szenario möchte das Opfer mit dem Ziel kommunizieren. Dafür benötigt es die Schicht 2 (MAC) Adresse des Ziels. Um diese zu ermitteln kommt die Neighbor

Discovery zum Einsatz. Der Angreifer antwortet schneller auf die Neighbor Solicitations, als die legitimen Eigentümer der IPv6 Adressen. So leitet er den Verkehr über sein System um.

Um beide Kommunikationsrichtungen anzugreifen, wird dieser Angriff wird sowohl in Richtung Opfer → Ziel als auch in die Richtung Ziel → Opfer durchgeführt.

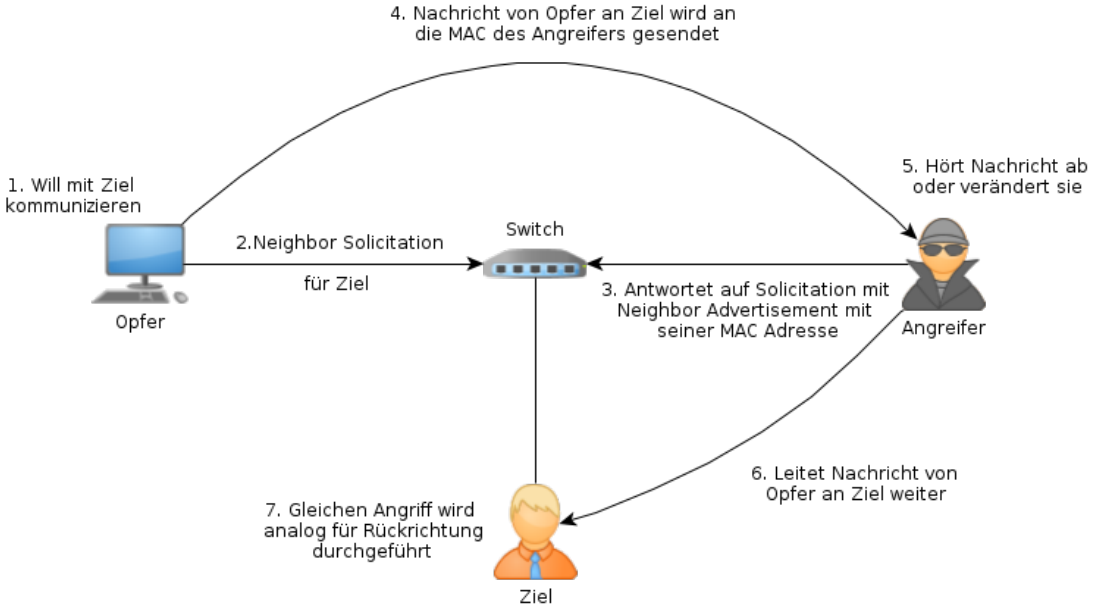


Abbildung 3.2.: Neighbor Cache Poisoning Angriff

Ein Angreifer könnte einen Neighbor Cache Poisoning Angriff beispielsweise mittels des Programms *parasite6* der THC-IPV6 Tool-Sammlung[1] durchführen. Da sich die Durchführung des Angriffs sehr einfach gestaltet, jeder Node angegriffen werden kann und alle drei Schutzziele verletzt werden, geht eine vergleichsweise hohe Gefahr von einem derartigen Angriff aus.

3.2. Neighbor Unreachability Detection

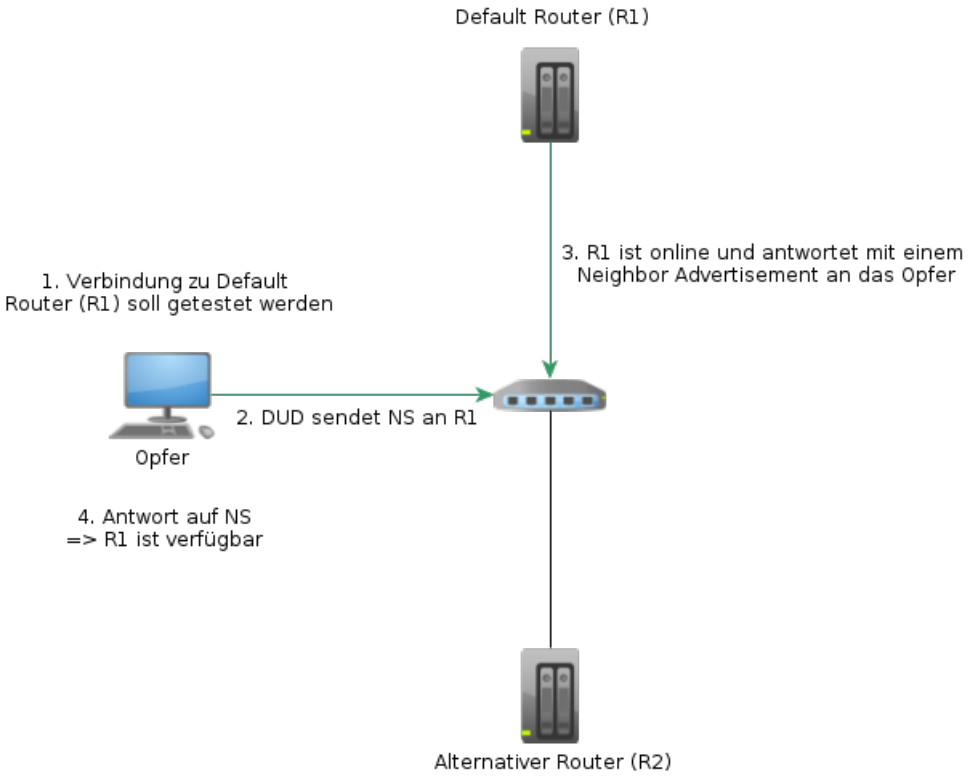
Die Neighbor Unreachability Detection (NUD) [RFC4861, Kap 7] dient der Erkennung, ob das Kommunikationsziel noch erreichbar ist. So soll vermieden werden, dass

[1] https://www.thc.org/thc-ipv6/ - Abruf am 04.12.2013

Nachrichten an nicht mehr erreichbare Nodes gesendet werden. Da bei der on-link-Kommunikation kein Router ICMP Fehlermeldungen zurückgeben könnte, würden Nachrichten an einen nicht mehr verfügbaren Node ins Leere laufen.

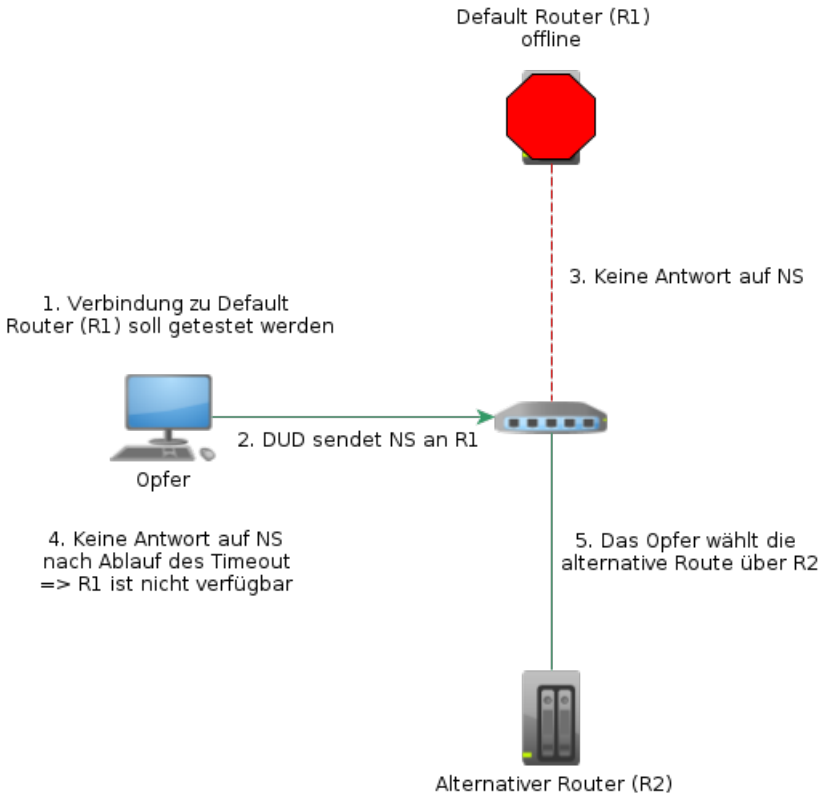
Um dies zu vermeiden, erlaubt die NUD die Erkennung nicht mehr erreichbarer Nodes, die noch einen Eintrag im Neighbor Cache besitzen. Dazu werden zum einen Information höherliegender Protokolle verwendet, beispielsweise solche über bestehende TCP Verbindungen.

Zum anderen werden, sofern keine Informationen der höher-liegenden Protokolle verfügbar sind, Neighbor Solicitations an den Node gesendet. Erfolgt eine Antwort in Form eines Neighbor Advertisements, so ist der Node weiterhin erreichbar (siehe Abb. 3.3). Andernfalls wird davon ausgegangen, dass das Ziel nicht mehr erreichbar ist. In diesem Fall ist die NUD fehlgeschlagen (siehe Abb. 3.4).



Der grüne Pfad symbolisiert die vom Opfer gewählte Route nach der NUD.

Abbildung 3.3.: Normalfall: Neighbor Unreachability Detection



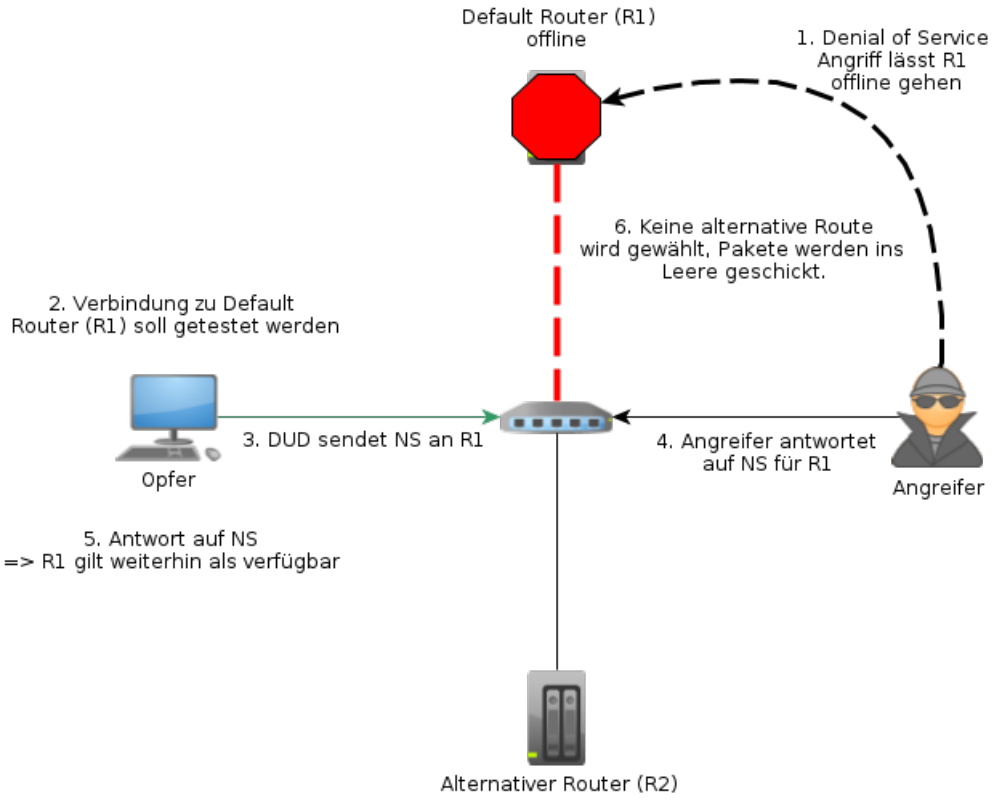
In diesem Fall ist der Router R1 ausgefallen. Der grüne Pfad symbolisiert die vom Opfer gewählte Route nach der NUD.

Abbildung 3.4.: Ausfall: Neighbor Unreachability Detection

Denial of Service Angriff

Ein Angreifer könnte die NUD dazu nutzen, die Opfer glauben zu lassen, dass ein Node weiterhin erreichbar ist. Dazu antwortet er mit Neighbor Advertisements auf die, durch die NUD angestoßenen Neighbor Solicitations für den nicht mehr erreichbaren Node. So würde das Opfer, im Glauben der Node sei weiterhin erreichbar, ohne dies zur Kenntnis zu nehmen, Nachrichten ins Leere senden. Es handelt sich dabei somit um einen Denial of Service Angriff.

Besonders wirksam ist der Angriff, wenn der bevorzugte Router des Opfers ausfällt (siehe Abb. 3.5). Einen derartigen Ausfall könnte ein Angreifer mittels eines DOS Angriffs herbeigeführt haben. In diesem Fall würde das Opfer normalerweise, nachdem die NUD ergeben hat, dass der bevorzugte Router nicht mehr erreichbar ist, alternative Router verwenden. Antwortet der Angreifer jedoch, stellvertretend für



In diesem Fall ist der Router R1 ausgefallen und der Angreifer für einen DOS Angriffdurch. Der grüne Pfad symbolisiert die vom Opfer gewählte Route nach der NUD.

Abbildung 3.5.: DOS Angriff mittels Neighbor Unreachability Detection

den ausgefallenen Router, mit entsprechenden Neighbor Advertisements, so würde die NUD des Opfers weiterhin den Router als erreichbar erkennen. Das Opfer würde für alle Nachrichten an off-link Nodes weiterhin den ausgefallenen Router verwenden. Somit würden die Nachrichten ins Leere gesendet werden, statt an einen alternativen Router. Es wäre ein Denial of Service herbeigeführt und das Opfer könnte nicht mit Zielen kommunizieren, die off-link sind.

Werden Protokolle höherer Schichten zur NUD verwendet, könnte der Angreifer beispielsweise TCP ACK Nachrichten senden, um das Opfer im Bezug auf die Verfügbarkeit des Nodes zu täuschen. Dies setzt jedoch Fehler bei der Implementierung der höheren Protokollschichten voraus, da beispielsweise TCP ACKs nur im Kontext einer Verbindung überhaupt akzeptiert werden sollten. Dieses Szenario wird hier nicht weiter betrachtet, da das Problem in diesem Fall nicht bei NDP sondern in der Implementierung der höheren Protokollschichten liegt. Ein konkreter IPv6-Bezug ist

somit nicht gegeben.

3.3. Router Discovery

Router Solicitations und Advertisements erlauben es Informationen über verfügbare Router, mittels des NDP Protokolls, anzufordern und bekannt zu machen. Ein Router sendet dabei periodisch Router Advertisements, in denen er sich als Router bekannt macht und Informationen zu den von ihm bedienten Präfixen ausliefert.

Anhand dieser Informationen kann einerseits bestimmt werden, welche IP Adressen welcher Präfixes sich direkt auf dem Link befinden und welche geroutet werden müssen. Mittels der Router Advertisements erhalten die Nodes außerdem die, für die Generierung globaler IPv6 Adressen notwendigen, Netzwerkpräfixe.

[RFC6106] beschreibt, wie sich mittels Router Advertisements Informationen über verfügbare DNS Server verteilen lassen. Auch ohne die Verwendung von DHCP lassen sich so Informationen über DNS Server bekanntgeben.

Will ein Node nicht auf ein periodisches Router Advertisement warten, so kann er per Multicast eine Router Solicitation senden. Auf diese sollten dann alle verfügbaren Router im Netz mit einem Router Advertisement antworten.

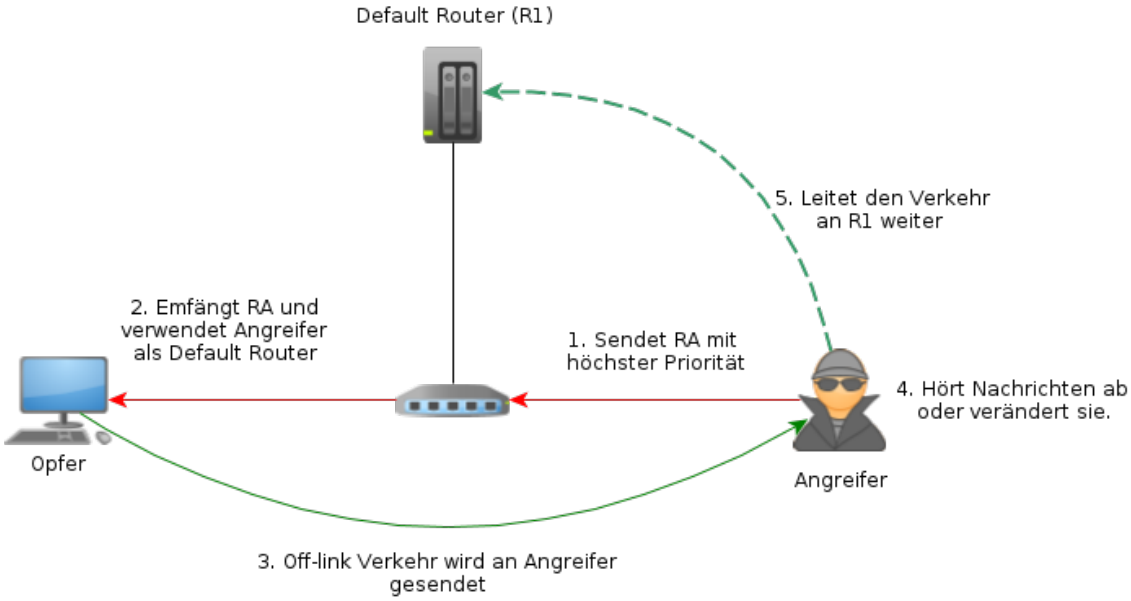
Auch bei der Router Discovery existieren standardmäßig keine Schutzmaßnahmen, die verhindern, dass sich ein Angreifer als Router ausgibt und unautorisiert Router Advertisements versendet. Zusätzlich zu dem Versenden von Router Advertisements ohne vorherige Router Solicitation, ist es dem Angreifer auch möglich auf jegliche Router Solicitations zu antworten.

Man-in-the-Middle Angriff

Wird der Angreifer von einem Opfer als Standardgateway gewählt, so wird jeglicher off-link-Verkehr über das von ihm kontrollierte System geleitet. Er hat volle Kontrolle über diesen Verkehr des Opfers. Nun gibt es zwei Möglichkeiten wie der Angreifer damit umgehen kann.

Zum einen könnte er den Verkehr abhören, möglicherweise verändern und an einen legitimen Router weiterleiten. So entstehen ein typisches Man-in-the-middle-Szenario (siehe 2.4.3).

Zum anderen könnte er den Verkehr lediglich verwerfen. Dieser Denial of Service Angriff (siehe 2.4.1) wird dann als *Blackholing* bezeichnet.



Der rote Pfeil zeigt den Weg des Router Advertisements (RA) vom Angreifer zum Opfer. Der grüne den Weg des über den Angreifer umgeleiteten Netzwerkverkehrs.

Abbildung 3.6.: Fake Router Angriff

Sollte die Route des Angreifers nicht von den Opfern gewählt werden, so gibt es noch immer die Möglichkeit den gewählten Standardgateway mittels eines Denial of Service Angriffs außer Kraft zu setzen. Ist der Standardgateway bei der Neighbor Unreachability Detection nicht mehr erreichbar, so würden Opfer den alternativen Router der Angreifers nutzen.

Ein Angriff bei dem sich der Anfreifer als Router ausgibt, kann beispielsweise mit dem Programm *fake_router6* aus der THC-IPV6 Sammlung[2] durchgeführt werden.

Da bei diesem Angriff direkt, mit nur einem Router Advertisement, alle an den Link angeschlossenen Nodes angegriffen werden können und weil er dem Angreifer so weitreichende Kontrolle ermöglicht, stellt sich dieser Angriff als sehr bedrohlich dar. Dies wird durch die einfache Durchführbarkeit noch weiter verstärkt.

[2]https://www.thc.org/thc-ipv6/ - Abruf am 04.12.2013

Perfomance Degrading

Ein alternativer Angriff kann durchgeführt werden, indem Router Advertisements im Namen des legitimen Routers versendet werden. Dabei kann ein Angreifer zahlreiche Konfigurationsparameter, die der Router an die Nodes weitergibt, modifizieren.

Beispielsweise kann er das Cur Hop Limit soweit reduzieren, dass die Pakete verworfen werden, bevor sie ankommen. Dies könnte zu einem Denial of Service führen (siehe [GONTND13, S. 43]).

Außerdem kann ein Angreifer dem Opfer eine falsche Maximum Transmission Unit (MTU) mitteilen. Diese könnte entweder sehr klein sein, was die Performance des Netzwerks negativ beeinflussen würde (siehe 2.4.2). Oder die MTU wäre zu groß, wodurch der Router möglicherweise die Pakete nicht annimmt. Dies könnte zum Paketverlust und Denial of Service führen. In der Regel wird jedoch eine ICMP Nachricht zurückgegeben, die besagt, dass die MTU des Routers überschritten wurde. Der Node würde in einem solchen Fall die MTU reduzieren, sodass die Pakete nicht mehr verworfen werden. Dennoch kann der Angriff die Performance und Stabilität des Netzes negativ beeinflussen.

Letztlich kann der Angreifer dem Opfer mittels der *M* und *O* Flags in den Router Advertisements mitteilen, dass dieses einen DHCPv6 Server zur Adresskonfiguration verwenden soll, siehe Abschnitt 3.5. So kann eine Ausgangssituation für die Durchführung weiterer Angriffe mittels DHCPv6 geschaffen werden.

3.4. Duplicate Address Detection

Bei der Duplicate Address Detection (DAD) handelt es sich um einen Mechanismus, welcher immer dann zum Tragen kommt, wenn einer Netzwerkschnittstelle eine neue IPv6 Adresse zugewiesen werden soll. Mit ihr wird überprüft, ob die neu zuzuweisende Adresse nicht schon im LAN vorhanden ist. Nur wenn dies nicht der Fall ist, wird der Schnittstelle die Adresse zugewiesen.

Dazu wird eine Neighbor Solicitation (NS) für die zuzuweisende IPv6 Adresse gesendet. Wurde diese Adresse bereits einem Node des Links zugewiesen, so antwortet dieser mit einem Neighbor Advertisement. In diesem Fall ist die Adresse ein Duplikat und darf nicht zugewiesen werden. Wird innerhalb eines festen Intervalls kein

Neighbor Advertisement empfangen, so kann davon ausgegangen werden, dass die Adresse noch nicht verwendet wird. Sie kann der Schnittstelle zugewiesen werden.

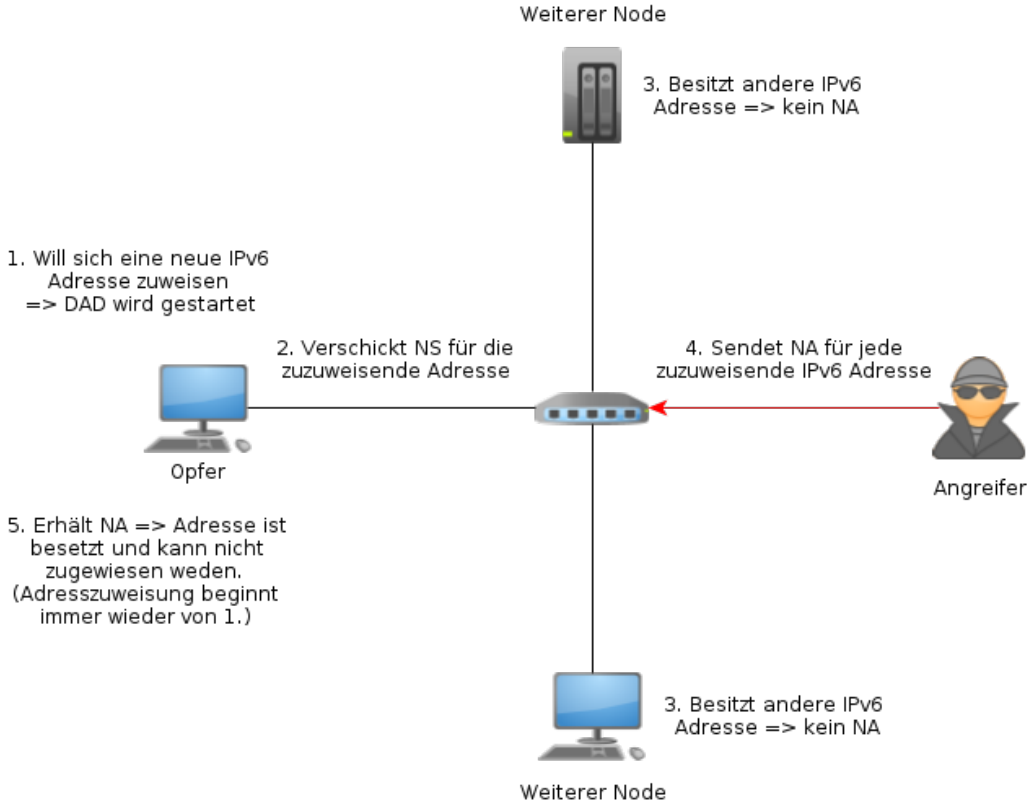


Abbildung 3.7.: Duplicate Address Detection DOS Angriff

Denial of Service Angriff

Der Mechanismus der DUD kann von einen Angreifer für einen Denial of Service Angriff ausgenutzt werden. Er antwortet dabei auf jegliche Neighbor Solicitations mit einem Neighbor Advertisement, unabhängig davon ob er die Adresse verwendet oder nicht.

Verbindet ein Opfer sein Endgerät mit dem Netz und möchte sich eine Adresse zuweisen, so wird die Zuweisung immer fehlschlagen, da die DAD alle Adressen als Duplikat ablehnt. Auch bei der Wahl alternativer Adressen schlägt die DAD wegen des Angriffs fehl. Da sich das Opfer so keine IP Adresse zuweisen kann, ist es nicht in der Lage das IPv6 Netz zu verwenden. Somit ist ein Denial of Service eingetreten.

Zur Durchführung eines solchen Angriffs in der Praxis könnte ein Angreifer das Programm *dos-new-ip6* aus der THC-IPV6 Sammlung[3] verwenden.

3.5. DHCPv6

Mit DHCPv6 existiert eine zustandsbehaftete Möglichkeit zur Zuweisung von IPv6 Adressen und Konfigurationsparametern, die alternativ zur Stateless Address Autoconfiguration (SLAAC) eingesetzt werden kann. Dabei wird ein zentraler DHCPv6 Server verwenden, der den Nodes auf Anfrage Adressen und Konfigurationsparameter zuweist.

Obwohl DHCPv6 dem Management der Netzwerkkonfiguration dient und somit Einfluss auf die Sicherheit des gesamten Netzes hat, bietet es keine ausreichenden Sicherheitsmechanismen. Es existiert lediglich ein mittels eines geheimen Schlüssels abgesichertes Authentifizierungsverfahren, welches zudem keinem Standard folgt. Damit existiert keine in der Praxis nutzbare Möglichkeit der kryptografischen Absicherung des Protokolls. Es bleibt durch verschiedenste Angriffe verwundbar.

Ein Angreifer könnte einen eigenen DHCPv6 Server betreiben. Dieser könnte entweder sinnlose Parameter an die Opfer ausliefern, die dazu führen, dass die Netzwerkkommunikation gestört und ein Denial-of-Service herbeigeführt wird. Oder er liefert vom Angreifer präparierte Konfigurationsparameter, wie beispielsweise die Adressen von DNS- oder NTP-Servern aus.

Ein manipulierter DNS Server könnte falsche Namensauflösungen durchführen, sodass Namen auf IP Adressen des Angreifers abgebildet würden. Damit könnte der Angreifer Teile des Netzwerkverkehrs über unter seiner Kontrolle befindliche Systeme umlenken.

Manipulierte NTP Server könnten falsche Zeitinformationen ausliefern, sodass die Uhr des Opfers beispielsweise in die Vergangenheit zurückversetzt wird. Dies lässt sich für Angriffe auf kryptografische Systeme nutzen, die Zeitstempel beispielsweise für Validitätszeiträume von Zertifikaten verwenden. Ein solcher Angriff kann eingesetzt werden, um abgelaufene Zertifikate zu verwenden, die normalerweise abgelehnt würden. Auf diese Weise wäre es einem Angreifer möglich erbeutete aber abgelaufene Zertifikate dennoch zu verwenden. Abhängig von den eingesetzen Lösungen ermöglicht dies eventuell weiterführenden Angriffen auf die Nutzer des Netzes.

[3] https://www.thc.org/thc-ipv6/ - Abruf am 04.12.2013

Um diese Angriffe durchzuführen, müssen die Nodes zuerst dazu bewegt werden diesen DHCPv6 Server zu verwenden. Kommt ohnehin DHCPv6 in dem Netz zum Einsatz, so könnten mittels präparierter Neighbor Advertisements (Neighbor Cache Poisoning, siehe Abschnitt 3.1) die Anfragen an den legitimen Server auf den des Angreifers umgelenkt werden.

Wird noch kein DHCPv6 Server eingesetzt, so könnten Nodes mittels präparierter Router Advertisements (siehe Abschnitt 3.3) dazu bewegt werden, einen DHCPv6 Server zu verwenden. Dies kann mittels der *M* (Managed address configuration) oder *O* (Other configuration) Flags geschehen (siehe [RFC4861, S. 19]). Daraufhin würden Nodes mittels Multicast nach einem DHCPv6 Server suchen. Auf diese Anfragen könnte der Angreifer antworten und die Nodes damit zur Nutzung des von ihm betriebenen DHCPv6 Servers bringen.

4. Maßnahmen

Die in Kapitel 3 beschriebenen Angriffe auf das Neighbor Discovery Protokoll zeigen, dass ein Angreifer über viele Möglichkeiten verfügt, Schaden zu verursachen. Insbesondere in Netzen mit hohen Sicherheitsanforderungen ist es notwendig entsprechende Schutzmaßnahmen zu treffen. Solche Maßnahmen werden nachfolgend, abhängig von ihrem Typ kategorisiert betrachtet. Jede von ihnen wird kurz beschrieben und die mit ihr verbundenen Kosten sowie Nutzen aufgezeigt.

4.1. Layer 2 und Hardware

Zum Schutz vor Angriffen kann die Logik auf Schicht 2 des OSI Modells erweitert werden, sodass die Netzwerkinfrastruktur Angriffe unterbindet. Diese neuen Funktionen würden dabei jeweils in die Switches integriert werden. Auf der Netzwerkinfrastrukturebene gibt es mehrere Schutzfunktionen, die jeweils Schutz vor einem Teil der Angriffe bieten sollen.

4.1.1. RA-Guard

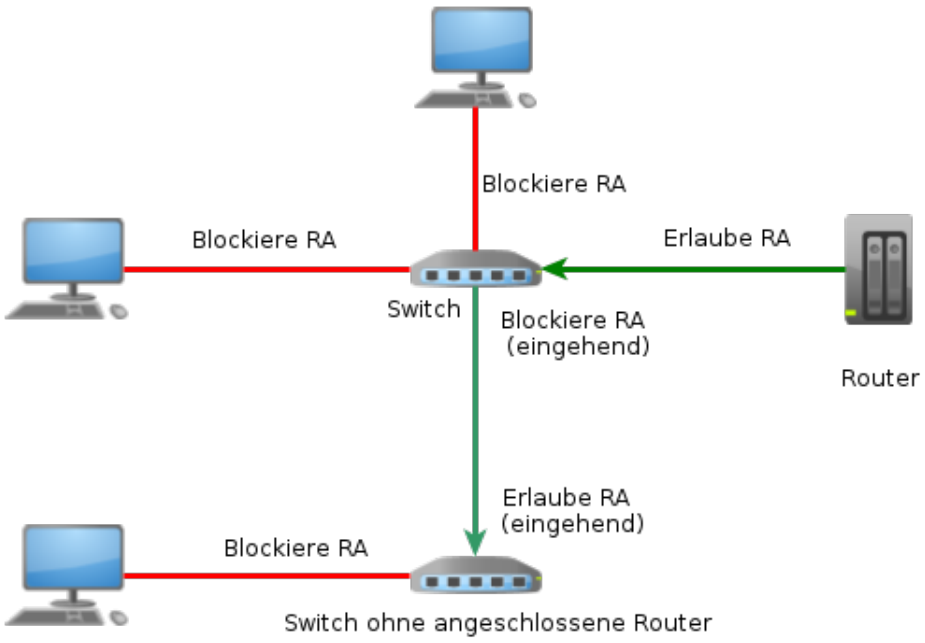
Der RA-Guard wurde in [RFC6105] standardisiert. Es handelt sich dabei um eine technische Schutzmaßnahme, welche in den Switches angesiedelt ist, an die die Endgeräte angeschlossen sind. Der RA-Guard ist eine Funktion um den Versand von Router Advertisements einzuschränken. So soll verhindert werden, dass Angreifer von beliebigen Ports eines Switches aus Router Advertisements versenden können. Die Maßnahme richtet sich somit gegen die in Abschnitt 3.3 beschriebenen Angriffe auf die Router Discovery.

Beschreibung

Beim RA-Guard wird für die Switchports definiert, ob an ihnen eingehende Router Advertisements akzeptiert werden dürfen. Da nur die eingehenden Nachrichten gefiltert werden, handelt es sich hier nur um eine Form der *Ingress*-Filterung. Wurden die Pakete durch den Switch nicht verworfen, so werden sie ganz normal weitergeleitet, ohne nochmals gefiltert zu werden, wenn sie den Switch verlassen.

Die Ports, an denen die Endgeräte angeschlossen sind, erlauben keine eingehenden Router Advertisements. Ein Angreifer, der ein Endgerät übernimmt oder sich an dessen Switchport anschließt, kann dementsprechend keine Router Advertisements an andere Nodes senden.

Die Ports an die Router angeschlossen werden, erhalten den *Trusted Port* Status. An diesen Ports wird keine Filterung eingehender Router Advertisements vorgenommen. Werden zwei RA-Guard-fähige Switches miteinander verbunden, so werden die für die Verbindung verwendeten Ports als *Trusted Ports* konfiguriert.



Die Pfeilrichtung gibt die regulären Wege von Router Advertisements in diesem Netz an, es sollten also nur Router Advertisements in diese Richtung erlaubt werden. Deswegen erlaubt der obere Switch an der Verbindung zum unteren auch keine eingehenden RAs. Diese Einstellung ist optional, verbessert jedoch die Sicherheit des Netzes.

Abbildung 4.1.: RA-Guard Einsatzszenario

Wurde die Switchting-Infrastruktur so entworfen, dass sie hierarchisch aufgebaut ist und Router nur zentral durch einen Pfad erreichbar sind, so kann auch bei dem in der Hierachie höher gelegenen Switch der Port so konfiguriert werden, dass eingehende Router Advertisements geblockt werden. Auf diese Weise kann verhindert werden, dass bei Kompromittierung eines Teil des Netzes, Router Advertisements in das restliche Netz gelangen. Diese Einstellung ist jedoch nur geeignet, wenn keine Querverbindungen existieren. Dementsprechend ist eine derartige Konfiguration, in gewachsenen oder nicht entsprechent entworfenen Netzen, nicht zum empfehlen.

RFC 6105 definiert auch eine zustandsorientierte Version des RA-Guard. Sie erlaubt es den Switch zuerst in einen Lernmodus zu versetzen, der erfasst auf welchen Ports Router Advertisements eingehen. Auf diesen Ports werden in der erzeugten Konfiguration eingehende Router Advertisements erlaubt. Der Lernmodus sollte aber mit Vorsicht eingesetzt werden. Andernfalls könnte ein Angreifer sich bereits im Netz befinden und Router Advertisements verschicken. Der Switch würde diesen Angriff als Normalzustand lernen und entsprechend würden auf dem Switchport des Angreifers weiterhin eingehende Router Advertisements erlaubt werden.

Auch in [RFC6105, Kap 6] wird ausdrücklich betont, dass bei der Verwendung der Lernfunktion sehr vorsichtig vorgegangen werden sollte, um nicht die Sicherheit des ganzen Netzes zu beeinträchtigen. Die erzeugte Konfiguration ist, um derartige Fehlkonfigurationen zu verhindern, auf jeden Fall sorgfältig von einen Administrator zu überprüfen. Dennoch kann die Lernfunktion die Konfiguration des RA-Guard durch die Administratoren merklich erleichtern.

Nutzen

Der RA-Guard schützt vor den in Abschnitt 3.3 beschriebenen Traffic Hijacking und Performance Degrading Angriffen, mittels gefälschter Router Advertisements. Dieser Schutz wird komplett durch die Switches umgesetzt. Er ist somit unabhängig von den Endgeräten und benötigt nicht die Implementierung speziellen Netzwerkprotokolle. Die Einrichtung der Schutzmaßnahme muss nur auf den Switches und nicht auf jedem Endgerät erfolgen, was die Administration erleichtert.

Außerdem bietet der RA-Guard den Vorteil, dass außer der Unterstützung durch die Switches, keine weiteren Anforderungen an die Infrastruktur oder Endgeräte gestellt werden.

Kosten

Um den RA-Guard effektiv einsetzen zu können, müssen alle Ports im Netz, an denen Endgeräte angeschlossen werden können, über die RA-Guard Funktion verfügen. Dafür muss jeder Switch über eine Managementfunktion und die entsprechenden Möglichkeiten zur Inspektion des Verkehrs verfügen.

Für die Erkennung und Filterung von Router Advertisements ist mehr Aufwand notwendig, als für das reine Switching. Eine Implementierung des RA-Guard ist nur in höherpreisigen Geräten von Herstellern wie Cisco und HP zu finden. Dies bedeutet, dass ein Austausch durch leistungsfähigere und teurere Geräte notwendig wäre, wenn nicht bereits entsprechende Switches verwendet werden. Damit verbunden wäre ein hoher finanzieller Aufwand für die entsprechende Hardware, sowie der personelle Aufwand der Administratoren für den Austausch großer Teile der Netzwerkinfrastruktur.

Es sollte bei der Einführung von RA-Guard dringend beachtet werden, dass alle Ports, von denen Router Advertisements erlaubt sind, auch physikalisch gesichert werden müssen. Dies betrifft insbesondere auch die Sicherheit der Verbindungen zwischen den Switches. Könnte sich ein Angreifer direkten Zugang zu einem solchen Port verschaffen, so wäre der RA-Guard umgangen und es könnten ungehindert Angriffe durchgeführt werden.

Zudem muss bei der Einführung bedacht werden, dass alle Switches, die untereinander mit Trusted Ports verbunden sind, mittels RA-Guard abgesichert sein müssen. Andernfalls könnten Angreifer über den ungesicherten Switch Router Advertisements in das Netz injizieren. Der Einsatz von RA-Guard für nur Teile des Netzes gestaltet sich deshalb schwer.

Wie in [CVE-2011-2395] beschrieben, können die Filter des RA-Guards, mittels Manipulation der Router Advertisements, umgangen werden. Ein Angreifer kann so trotz RA-Guard nahezu ungehindert Router Advertisements versenden. Betroffen von dieser Schwachstelle ist beispielsweise die Implementierung des Marksführers Cisco. Die Möglichkeiten des Umgehens werden in [RFC7113] weiter erläutert.

Zum Umgehen gibt es die Möglichkeit die NDP Nachricht so zu fragmentieren, dass der ICMPv6 Header nicht (vollständig) im ersten Paket enthalten ist. Da der Switch nicht in der Lage ist die Fragmente wieder zusammenzusetzen, kann er die Nachricht nicht als Router Advertisement erkennen und leitet sie weiter, anstatt sie

zu verwerfen.

Dieser Angriff kann dadurch verhindert werden, dass der Switch um eine *IP-Reassembly*-Funktion erweitert wird. Diese Funktion reassembliert IP Fragmente im Switch, um Router Advertisements erkennen zu können. Dies ist jedoch sehr aufwendig, da die Fragmente auf dem Switch zwischengespeichert werden müssen, wodurch die Hardwareanforderungen nochmals steigen. Eine derartige Funktion existiert zwar beispielsweise bei Cisco, jedoch hauptsächlich im Backbone Bereich. Sie ist quasi nicht in den Switches für Endgeräte anzutreffen.

Weil diese Lösung somit nicht als praktikabel angesehen werden kann, wurde mittlerweile der Standard so angepasst, dass die Fragmentierung von NDP Nachrichten verboten ist. Diese Anpassung wird in 4.1.4 noch genauer erläutert. Wird sie umgesetzt, würde kein Endgerät fragmentierte NDP Nachrichten akzeptierten, sodass der RA-Guard wieder ein wirksamer Schutz gegen gefälschte Router Advertisements wäre.

Da das Fragmentierungsverbot jedoch auf absehbare Zeit nicht in allen IPv6 Implementierungen umgesetzt werden wird, sollten kurzfristige Alternativen in Betracht gezogen werden. Ein Schutz vor der Fragmentierung von NDP Nachrichten kann durch Paketfilter auf Endgeräten realisiert werden. Bei Windows Endgeräten könnte mittels der Windows Firewall der NDP Verkehr nach fragmentierten Nachrichten gefiltert werden. Entsprechende Regeln lassen sich über die Domänenrichtlinien auf alle Endgeräten verteilen. Bei Linux könnte eine solche Filterung z.B. über *iptables* erfolgen. Dennoch kann so nur ein Teil der Endgeräte geschützt werden. Integrierte Systeme, wie Drucker, besitzen keine Möglichkeiten zur Paketfilterung und sind somit weiterhin angreifbar. Zudem ist die Verteilung entsprechender Regelsätze, insbesondere in heterogenen Umgebungen, recht aufwendig, sodass leicht Systeme übersehen werden können. Trotzdem können mittels Paketfiltern kurzfristig viele Systeme vor fragmentierten Router Advertisements geschützt werden.

Ende Januar 2014 wurde [RFC2460] durch [RFC7112] aktualisiert. Die Änderung schreibt vor, dass nun die komplette IPv6 Header Chain, also der IPv6 Header, alle Extension Header und der Header des Upper Layer Protocol (ULP) im ersten IP Fragment enthalten sein müssen. Dies vereinfacht die zustandslose Filterung von IPv6 Verkehr, da alle dazu notwendigen Informationen nun im ersten Fragment enthalten sein müssen. Ist der ULP Header nicht im ersten Fragment enthalten, so soll das Paket verworfen werden. Eine Reassemblierung ist durch die Änderung für

die Filterentscheidung nicht mehr notwendig.

Da es sich bei dem RA-Guard um eine Implementierung eines zustandslosen Filters handelt, hat die Änderung auch Auswirkungen auf den RA-Guard. Switches könnten nun Nachrichten verwerfen die Fragmentierung einsetzen, um der Untersuchung durch RA-Guard zu entgehen. Der Header des ULP, also in diesem Fall ICMPv6, muss dementsprechend im ersten Fragment enthalten sein, sodass der RA-Guard Router Advertisements erkennen kann. Wird diese Änderung in Zukunft in den Switches implementiert, so würde dies die Wirksamkeit des RA-Guard für alle Systeme stark verbessern. Ein Angreifer könnte den RA-Guard nicht mehr mittels geschickter Fragmentierung umgehen. In dem Fall wären auch Systeme, die noch immer fragmentierte NDP Nachrichten akzeptieren, durch den RA-Guard geschützt.

In [RFC7113, Kap 2.1] wurde ebenfalls festgestellt, dass einige Implementierungen des RA-Guard bei der Suche nach einer ICMPv6 Nutzlast (Router Advertisement) nicht die kompletten Kette der Extension Header untersuchen. So lassen sich mit Extension Headers präparierte Router Advertisements an dem RA-Guard vorbeischleusen. Diese Schwachstelle kann durch die standardkonforme Behandlung der Extension Headers vermieden werden. In den aktuellen Implementierungen großer Hersteller sollte dieses Problem zwar behoben sein, dies sollte dennoch vor der Einführung neuer Switches mit RA-Guard überprüft werden. Um ähnliche Schwachstellen zu vermeiden, ist es wichtig immer eine aktuelle Firmware auf den Switches zu verwenden.

Insgesamt schützt der RA-Guard nur vor Angriffen mittels Router Advertisements. Ein Schutz vor Angriffen mittels anderer Funktionen des Neighbor Discovery Protokolls, wie beispielsweise Neighbor Advertisements, ist nicht gegeben. Somit werden weitere Schutzmaßnahmen notwendig um alle beschriebenen Angriffe zu verhindern.

4.1.2. FCFS-SAVI

Das in [RFC6620] standardisierte FCFS-SAVI (First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses) dient zum Schutz vor IP Paketen mit gefälschten Quelladressen. Kann ein Angreifer IP Pakete mit gefälschter Quelladresse versenden, so kann er auch Neighbor Advertisements im Namen beliebiger Nodes versenden. Auf diese Weise kann er die in Abschnitt 3.1 beschriebenen Angriffe durchführen. Genau diese Adressfälschung und die daraus

resultierenden Angriffe soll FCFS-SAVI verhindern.

Auf Basis der gesendeten Neighbor Discovery Nachrichten, lernt der Switch bei FCFS-SAVI die mit seinen Ports assoziierten IPv6 Adressen. Nur IP Pakete deren Quelladresse so mit dem Port assoziiert ist, werden von dem Switch akzeptiert und weitergeleitet. Pakete mit gefälschter Quelladresse werden herausgefiltert und können so ihr Ziel nicht erreichen.

Beschreibung

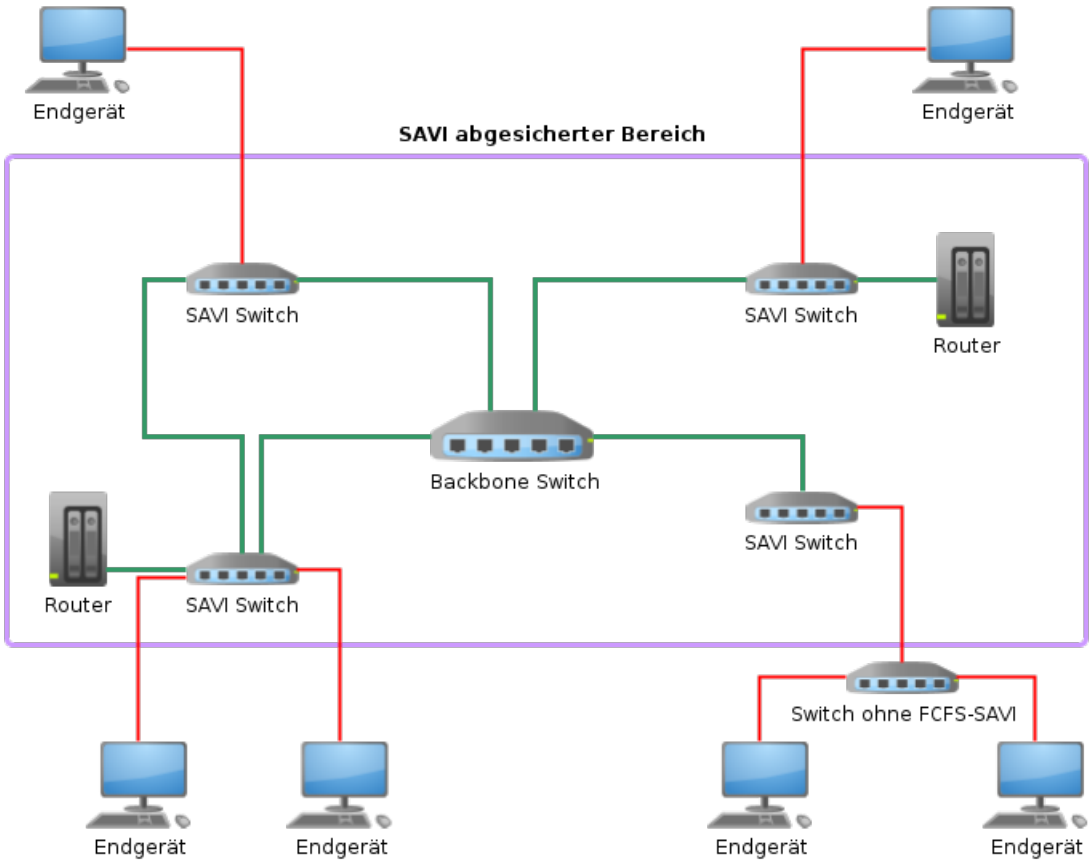
Die IPv6 Adressen werden bei FCFS-SAVI jeweils an einen Sicherheitsanker gebunden. Das bedeutet, dass nur IP Pakete deren Quelladresse an dem Sicherheitsanker gebunden ist, versendet werden können. Grundsätzlich wird hier der physikalische Port des Switches als Sicherheitsanker verwendet. Theoretisch wäre auch die Bindung an die Schicht 2 Adresse (z.B. MAC) denkbar. Da sich diese jedoch leicht verändern lässt, sieht der RFC ausschließlich die Nutzung der physikalischen Ports als Sicherheitsanker vor. Es entsteht eine Tabelle, die definiert welche IPv6 Quelladressen an dem physikalischen Port akzeptiert werden.

FCFS-SAVI kombiniert durch die Binding-Tabelle Informationen verschiedener Protokollschichten. Die IPv6 Quelladresse der Schicht 3 wird mit Informationen der Schicht 2, wie dem verwendeten Switchport, kombiniert. So kann der IPv6 Verkehr mit Hilfe der Informationen niedrigerer Protokollschichten gefiltert werden.

Bei FCFS-SAVI werden zwei Typen von Switchports unterschieden, die *Validating Ports* und die *Trusted Ports*. Auf den Validating Ports wird eine Validierung, auf Basis der Binding-Tabelle, durchgeführt. Auf den Trusted Ports sind jegliche Quelladressen erlaubt. Sie kommen beispielsweise zur Verbindung mehrerer FCFS-SAVI Switches zum Einsatz.

Bei der Verbindung von FCFS-SAVI Switches wird davon ausgegangen, dass den FCFS-SAVI Switches sowie den Uplinks vertraut werden kann. So wird ein Bereich erzeugt, dessen eingehender Netzwerkverkehr mittels SAVI gefiltert wird. Somit handelt es sich um eine *Ingress*-Filterungsmaßnahme.

Switches, die FCFS-SAVI unterstützen, besitzen eine Binding-Tabelle, in der Assoziationen zwischen physikalischen Ports und IPv6 Adresse gespeichert werden. In den meisten Fällen darf jeder Port ein Maximum von beispielsweise 5 IPv6 Adressen



Grüne Verbindungen sind solche denen vertraut wird, also mittels Trusted Ports. Rote Verbindungen stellen nicht vertrauenswürdige Verbindungen dar, sie bedürfen einer Überprüfung mittels eines Validating Ports.

Abbildung 4.2.: FCFS-SAVI Anwendungsbeispiel

binden. So kann verhindert werden, dass ein Angreifer an einem Port einen Duplicate Address Detection DOS Angriff durchführt oder zu viele Ressourcen in der Binding-Tabelle beansprucht. Von dem Switch nur IP Pakete weitergeleitet, deren Quelladresse an den Switchport gebunden ist, auf dem diese eintreffen.

Wenn sich ein Node versucht eine neue Adresse zuzuweisen, führt er zuerst die Duplicate Address Detection durch. Dabei versendet er eine Neighbor Solicitation, um zu erfahren ob bereits ein anderer Node die zuzuweisende Adresse verwendet. Die Neighbor Solicitation lässt der Switch passieren. Erfolgt keine Antwort und ist die Adresse auch nicht in der Binding-Tabelle vorhanden, darf der Node diese verwenden. In diesem Fall erstellt der Switch eine neue Assoziation zwischen Port und IPv6 Adresse.

Ist die maximale Anzahl der an einen Port gebundenen Adressen überschritten, wird die älteste Bindung verworfen. Das Neighbor Advertisement auf das bei diesem Prozess gewartet wird, kann ausschließlich von einem Inhaber der Adresse oder über einen Trusted Port des Switches kommen.

Der Switch kann auch Neighbor Solicitations an einen Port senden, um herauszufinden ob noch ein Node mit entsprechender IPv6 Adresse angeschlossen ist. Erfolgt keine Antwort, so kann davon ausgegangen werden, dass diese Adresse nicht mehr verwendet wird. Diese Funktion kann verwendet werden um veraltete Einträge aus der Binding-Tabelle zu entfernen.

Nutzen

FCFS-SAVI stellt sicher, dass ein Node eine Quelladresse nur nutzen kann, wenn diese an seinen Switchport gebunden wurde. So kann das Versenden gefälschter Neighbor Advertisements und der damit verbundene Traffic Hijacking Angriff (siehe Abschnitt 3.1) verhindert werden. Im gleichen Zug wird auch der Duplicate Address Detection DOS Angriff verhindert, da die gefälschten Neighbor Advertisements des Angreifers vom Switch gefiltert werden würden.

Für die Endgeräte ist der Einsatz von FCFS-SAVI komplett transparent, da die Maßnahme ausschließlich die vorhandenen Mittel des Neighbor Discovery Protocol verwendet. Somit sind keine Einstellungen, Veränderungen oder Installationen auf den Endgeräten notwendig, sodass die Einführung für die Netzwerk- und Systemadministratoren erleichtert wird. Für die Einführung ist somit nur die Anpassung der Konfigurationen der Switches notwendig.

Kosten

Der maßgebliche Nachteil bei FCFS-SAVI ist, dass alle Switchen an denen Endgeräte angeschlossen sind FCFS-SAVI unterstützen müssen. Die Einbindung eines nicht SAVI-fähigen Switches über einen Validating Port eines FCFS-SAVI-fähigen Switches ist grundsätzlich möglich. Jedoch ist die Anzahl der an ihn anschließbaren Nodes stark limitiert. Dies liegt daran, dass die maximale Anzahl an IPv6 Adressen, die an den Validating Port gebunden werden können, limitiert ist. Ein solches Szenario erscheint somit nur als Übergangslösung sinnvoll.

Bisher gibt es noch kaum Geräte die FCFS-SAVI unterstützen. Da es sich um eine wenig nachgefragte Funktion handelt und auch zusätzliche Resourcen für die Binding Tabelle benötigt werden, sind die verfügbaren Switches vergleichsweise teuer. Mitunter liegt dies jedoch auch darin begründet, dass der Standard sehr neu ist und es einige Zeit dauern könnte, bis er von den Herstellern aufgegriffen wird. Die Einführung von FCFS-SAVI würde dementsprechend hohe finanzielle und personelle Kosten verursachen, da damit zu rechnen ist, dass die meisten Switches ausgetauscht werden müssen.

Bei falscher Implementierung der Binding-Tabelle oder fehlenden Limits für die Einträge eines Ports, könnte es zu einem Denial of Service kommen. Ein Angreifer könnte versuchen die Binding-Tabelle mit eigenen Einträgen zu füllen und so die alten Einträge zu verdrängen. Werden dadurch die IPv6 Adressen der an anderen Ports angeschlossenen Endgeräte wieder aus der Tabelle entfernt, können diese nicht mehr kommunizieren. Außerdem kann ein Angreifer die nicht mehr gebundenen Adressen vereinnahmen und Nachrichten in ihrem Namen versenden. Dieser Problematik kann jedoch durch die Konfiguration fester Kontingente und Limitierungen für jeden Port vorgebeugt werden.

Kommen Privacy Extensions zum Einsatz, muss überprüft werden ob der Switch genug IPv6 Adressen an den Port binden kann, um auch die bereits veralteten, jedoch noch in Verwendung befindlichen, Quelladressen (deprecated adresses) speichern zu können. Andernfalls können Funktionsproblemen und Beeinträchtigungen der Verfügbarkeit auftreten.

Abschließend ist zu FCFS-SAVI zu sagen, dass es nicht in einer Umgebung gleichzeitig mit SEND zum Einsatz kommen sollte. Dies wäre auch unnötig, da beide gegen Adressdiebstahl durch einen Angreifer schützen. Die Inkompatibilität liegt darin begründet, dass der SAVI-fähige Switch Neighbor Solicitations (DAD_NS) mit den Absenderadressen der angeschlossenen Nodes verschickt. Dies ist mit SEND nicht möglich, da der Schlüssel für die zur Adresse passende Signatur nicht vorhanden ist.

Für die Benutzung von Source Address Validation in Kombination mit SEND existiert bereits ein Draft für einen RFC [SENDSavi]. Das in ihm beschriebene Verfahren ist somit der Kombination von FCFS-SAVI und SEND vorzuziehen. Mangels praktischer Anwendung soll diese Lösung hier jedoch nicht weiter beschrieben werden.

4.1.3. Cisco IPv6 First-Hop Security

Cisco Switches bieten einen ganzen Satz eigener Funktionen, die der Absicherung des Links bei IPv6 dienen. Dies umfasst eine Implementierung des RA-Guard (siehe 4.1.1). Zusätzlich ergänzen Funktionen wie der IPv6 Destination Guard, der IPv6 Source Guard, der IPv6 Prefix Guard und der DHCPv6 Guard das Portfolio.

Diese Features verwenden das IPv6 Snooping Feature, welches passiv den Netzwerkverkehr mithört und daraus die mit den Ports assoziierten IPv6 Adressen ableitet. Dadurch können Assoziationen zwischen eingehendem Netzwerkport, IPv6 Adresse und auch Adressen der Schicht 2 (z.B. MAC) erzeugt werden. Diese werden in der Binding-Tabelle des Switches abgelegt. Diese wird dann wiederum von den anderen Features genutzt, um den Link abzusichern. Zusätzlich kann der Administrator auch statische Einträge in diese Tabelle hinzufügen, wenn dies notwendig ist.

IPv6 Destination Guard

Der IPv6 Destination Guard lässt nur Neighbor Solicitations für Adressen zu, die sich in der Binding-Tabelle befinden, also an einem der Ports gebunden wurden. So soll das Fluten des Netzes mit Neighbor Solicitations verhindert werden. Außerdem lassen sich mittels dieser Funktion IPv6 Nachrichten anhand des Ziels herausfiltern.

IPv6 Source Guard

Bei dem IPv6 Source Guard wird die IPv6 Binding-Tabelle des Geräts dazu verwendet, um für die einzelnen Netzwerkports zu definieren, welche Quelladressen für eingehende Nachrichten erlaubt sind. Zur Filterung des eingehendes Verkehrs kommen die *IPv6 port-based access control list* (PACL)[1] zum Einsatz. So kann verhindert werden, dass ein angeschlossener Node Quelladressen verwendet, die nicht an seinen Port gebunden sind.

Die Funktionsweise des Source Guard erinnert stark an das in 4.1.2 beschriebene FCFS-SAVI. Zwar bezieht sich Cisco nirgendwo auf den [RFC6620] und gibt an die beschriebene Lösung zu implementieren. Jedoch sind mehrere Cisco Mitarbeiter

[1] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-sy/sec-data-acl-15-sy-book/ip6-pacl-supp.html - Abgerufen am 10.01.2014

unter den Autoren des FCFS-SAVI Standards. Die fehlende Erwähnung von FCFS-SAVI mag auch daran liegen, dass die Standardisierung von FCFS-SAVI erst kurze Zeit zurück liegt und Cisco schon länger über den IPv6 Source Guard verfügt.

DHCPv6 Guard

Der DHCPv6 Guard ermöglicht es, analog zum RA-Guard, nur auf bestimmten Ports eingehende Servernachrichten eines DHCPv6 Servers zu erlauben. DHCPv6 Nachrichten von nicht dazu autorisierten Ports können verworfen werden. Dieses Feature richtet sich gegen den in Abschnitt 3.5 vorgestellten Angriff auf das Netz, mittels eines vom Angreifer präparierten DHCPv6 Servers.

IPv6 Prefix Guard

Der IPv6 Prefix Guard bietet die Möglichkeit der Filterung nach dem Netzwerkpräfix. So können Pakete verworfen werden, deren IPv6 Quelladresse zwar korrekt ist und vom IPv6 Source Guard zugelassen wurde, deren Präfix jedoch nicht den Vorgaben der Netzwerktopologie entspricht. So kann verhindert werden, dass IPv6 Adressen anderer Netze gewählt und so Nachrichten in deren Namen verschickt werden.

Nutzen

Die Schutzmaßnahmen ermöglichen es, das Netz gegen alle der in Kapitel 3 beschriebenen Angriffe abzusichern.

- Mit dem RA-Guard existiert wie schon in 4.1.1 beschrieben eine Schutzmaßnahme gegen gefälschte Router Advertisements.
- Der IPv6 Source Guard schützt vor Neighbor Cache Poisoning sowie vor Denial-of-Service-Angriffen mittels der Duplicate Address Detection oder Neighbor Unreachability Detection.
- Mit dem IPv6 Prefix Guard kann verhindert werden, dass falsche Netzwerkpräfixe zum Einsatz kommen. So können manche Parameter Manipulation Angriffe abgewehrt werden.
- Der IPv6 Destination Guard schützt vor der Überflutung des Netzes mit NDP Nachrichten.

Für den Einsatz der Maßnahmen werden lediglich Switches mit den entsprechenden Funktionen, die Cisco „IPv6 First-Hop Security Features“ nennt, benötigt. Jedes standardkonforme IPv6 Endgerät kann, ohne weitere Einrichtung oder spezielle Software, in einem so geschützten Netz verwendet werden.

Kosten

Es muss eine Bindung an den Hersteller Cisco erfolgen, da nur dessen Switches über die entsprechenden Funktionen verfügen. Für den Einsatz muss eine homogene Cisco Switching Infrastruktur existieren oder aufgebaut werden. So besteht zukünftig eine Abhängigkeit von Cisco. Es können zukünftig nur Switches von Cisco angeschafft werden, sodass die Flexibilität bei Anschaffungen negativ beeinflusst wird.

Insgesamt sind die Maßnahmen nur wirksam, wenn alle über Trusted Ports verbundenen Switches sie einsetzen. Potentielle Angriffspunkte stellen somit ungesicherte Switches an Trusted Ports dar. Da diese Switches keine Validierung durchführen, könnte ein Angreifer so manipulierte Pakete in die restlichen Teile des Netzes senden. Ein flächendeckender Einsatz der Maßnahmen ist somit unumgänglich.

Die Switches mit den „IPv6 First-Hop Security Features“ sind vergleichsweise teuer, da die neuen Funktionen zuerst in die leistungsfähigen Switches integriert wurden. Durch die notwendigen Neuanschaffungen und aufwendigen Migrationen kann es somit zu hohen personellen und finanziellen Kosten für die Einführung kommen.

4.1.4. Fragmentierungsverbot für Neighbor Discovery

[CVE-2011-2395] beschreibt, dass sich die Schutzmaßnahmen des RA-Guards, beispielsweise in der Cisco Implementierung, mittels Fragmentierung der Router Advertisements umgehen lassen. So kann ein Angriff trotz der Verwendung des RA-Guard nahezu ungehindert durchgeführt werden. Die Möglichkeiten des Umgehens der Filterung werden in [RFC7113] im Detail erläutert.

In [CVE-2011-2395] wird beschrieben, dass die Fragmentierung einer ICMP Nachricht in mehrere IP Fragmente, dazu genutzt werden kann, um den Überprüfungen des RA-Guard zu entgehen. IPv6 sieht das Zusammenfügen der IP Fragmente erst wieder am Ziel vor. Würde der Switch die Reassemblierung umsetzen, müsste er noch

nicht zusammengefügte Pakete zwischenspeichern, was zu einem hohen Resourcenaufwand führen würde. Dementsprechend musste eine alternative Lösung gefunden werden, um dem Problem der Fragmentierung zu begegnen.

Mittels des von Fernando Gont eingebrachten [RFC6980] wurden die RFCs [RFC4861] und [RFC3971] so aktualisiert, dass die Fragmentierung von IPv6 in allen Neighbor Discovery Nachrichten nun verboten ist.

Für Fragmentierung von NDP Nachrichten existiert kein praktischer Anwendungsfall. Deshalb hat das neue Verbot keinen Einfluss auf die legitime Funktionalität des Netzes. Dass keine Fragmentierung auftritt, liegt darin begründet, dass NDP Nachrichten sehr klein sind und somit keine Fragmentierung benötigen. Eine Ausnahme bilden nur große Zertifikate die beim Einsatz von SEND über das NDP Protokoll übertragen werden. Für sie definiert der RFC 6980 eine explizite Ausnahme.

Würde das Verbot umgesetzt, so könnten fragmentierte Router Advertisements zwar den mit RA-Guard gesicherten Switch passieren, würden jedoch von den Endgeräten verworfen werden. Der Angriff ist somit nicht mehr möglich.

Nutzen

Diese Änderung ermöglicht es einfach und elegant die Probleme mit fragmentierten Neighbor Discovery Nachrichten zu beheben. Dadurch stellt der RA-Guard wieder eine effektive Schutzmaßnahme dar. Außerdem ist dieser Lösungsansatz für die Netzwerkhardware sehr günstig, da keine zusätzlichen Funktionen implementiert werden müssen. Auch ein Update für bestehende Switches ist nicht notwendig, sodass alle Geräte die bisher den RA-Guard unterstützen, mit der Änderung ohne Probleme weiter verwendet werden können.

Kosten

Das Hauptproblem liegt darin, dass die Änderung am Neighbor Discovery Protokoll erst Ende 2013, also vor sehr kurzer Zeit geschah. Besonders eingebettete Systeme mit einem IPv6 Stack erhalten mitunter niemals ein Update, sodass davon ausgegangen werden kann, dass die Änderungen in naher Zukunft noch nicht auf allen Geräte umgesetzt sein werden. Diese Geräte wären dann durch Angriffe mittels fragmentierter NDP Nachrichten weiterhin verwundbar.

Die Änderung muss zuerst in die jeweiligen Betriebssystem übernommen und dann auch noch mittels entsprechender Systemupdates auf den Endgeräten eingespielt werden. Aktuell sind die Änderungen auch in vielen verbreiteten Betriebssystemen noch nicht umgesetzt. Sodass es wohl noch einige Zeit dauern wird, bis von den meisten Systeme keine fragementierten NDP Nachrichten akzeptiert werden.

4.2. Kryptografische Schutzmaßnahmen

4.2.1. IPsec

IPsec war ursprünglich eines der wesentlichen neuen Features von IPv6, wurde jedoch zwischenzeitig auch auf IPv4 portiert. Es ermöglicht den Aufbau gesicherter Netzwerktunnel auf IP-Ebene. Zur Absicherung des Neighbor Discovery Protocol wäre es auch denkbar, die Nachrichten zwischen zwei Nodes immer über einen verschlüsselnden und authentifizierenden Tunnel zu senden.

Nutzen

Da IPsec lange Zeit verpflichtend von jeder der IPv6 Implementierungen unterstützt werden sollte, und IPsec eine wichtige Rolle für die Sicherheit zugeschrieben wurde, ist eine IPsec Unterstützung in den meisten Protokollimplementierungen von IPv6 zu finden. Auf den meisten eingebetteten Systemen existiert jedoch keine Implementierung von IPsec. Dies ist darin begründet, dass die kryptografischen Operationen für die eingesetze Hardware zu aufwendig wären. Außerdem gibt es bisher auch keinen Bedarf für IPsec auf derartigen Systemen.

IPsec setzt eine kryptografisch starke Verschlüsslung und eine Authentifizierung mittels eines Message Authentication Codes ein, sodass Manipulation und Fälschung entsprechender NDP Nachrichten entgegengewirkt werden könnte. Ein Angreifer der sich an einen Switchport anschließt, könnte weder manipulativ in bestehende Kommunikation eingreifen, noch eigene gefälschte NDP Nachrichten versenden. Er besitzt nicht den geheimen Schlüssel um sich als authentisierter Teil der Gruppe auszugeben und so NDP Nachrichten zu versenden.

Kosten

Das Hauptproblem stellt hier das Schlüsselmanagement dar, denn hierfür wird bei IPsec das Internet Key Exchange Protocol (IKE) eingesetzt. IKE benötigt für seine Funktion eine zugewiesene IP Adresse. Da bei der Zuweisung einer IPv6 Adresse bereits eine DAD durchgeführt werden muss, entsteht hier ein Henne-Ei-Problem. Die Adresszuweisung benötigt eine DAD mittels NDP, NDP sollte über IPsec abgesichert werden, und IPsec benötigt wiederum für die Schlüsselverteilung eine IP Adresse.

Ein Lösungsansatz für die Problematik bei der Adresszuweisung wäre die Implementierung von IKE auf ICMPv6 mit Multicast Paketen. Bei einer derartigen Umsetzung wäre eine Schlüsselabfrage und der Aufbau einer Security Association ohne einge zugewiesene IPv6 Adresse möglich.

Alternativ zur Verwendung von IKE ist auch die manuelle Konfiguration aller Security Associtations möglich. Dies skaliert jedoch in größeren, sich dynamischen verändernden Netzen nicht, da der Konfigurationsaufwand zu hoch wäre.

Zudem werden viele NDP Nachrichten über Multicast gesendet. Dies kann mit IPsec nur schlecht abgebildet werden. Da symmetrische Kryptografie zum Einsatz kommt, müssten alle Teilnehmer der Multicast-Gruppe den gleichen symmetrischen Schlüssel verwenden. Somit bedeutet der Besitz des Schlüssels nur, dass der Benutzer Mitglied der Multicast-Gruppe ist, seine individuelle Identität kann jedoch nicht nachvollzogen werden. Jedes Mitglied der Gruppe könnte im Namen von anderen Mitgliedern ungehindert Nachrichten versenden.

Da im Regelfall die Kompromittierung über ein bereits in die Multicast-Gruppe eingebundenes Endgerät erfolgt, wäre auch der Angreifer im Besitz des geheimen Schlüssels. Er könnte dann ungehindert alle beschriebenen Angriffe gegen die restlichen Mitglieder durchführen.

Praktisch findet die Absicherung von NDP mittels IPsec noch keine Anwendung. Dies ist darin begründet, dass noch keine Lösung für das Henne-Ei-Problem bei der Adresszuweisung existiert. Außerdem stellt die individuelle Authentisierung der Nodes bei Multicast Nachrichten ein bisher nicht gelöstes Problem dar. Bemühungen oder Ansätze zur Implementierung von IKE auf ICMP statt UDP finden aktuell nicht statt.

4.2.2. SEcure Neighbor Discovery

Die zugewiesenen IPv6 Interface Identifier, also letzten 64 Bits einer IPv6 Adresse, werden in einer SEND [RFC3971] Umgebung mittels Cryptographically Generated Addresses (CGA) [RFC3972] kryptografisch, auf Basis eines RSA Schlüsselpaars, generiert. Jeder Node erhält dabei ein eigenes RSA Schlüsselpaar. Um bei der Neighbor Discovery zu beweisen, dass der Absender wirklich der Besitzer der entsprechenden IPv6 Adresse ist, wird eine kryptografische Signatur mittels des, der Adresse zugrunde liegenden, privaten RSA Schlüssels verwendet.

Insbesondere um Router zum Versand von Router Advertisements zu autorisieren, kommt ein zentraler Vertrauensanker zum Einsatz. Durch Zertifikatsketten zum zentralen Vertrauensanker kann sichergestellt werden, dass Router Advertisements und Redirects nur von dazu autorisierten Routern versendet werden. Kann ein Router keine solche Zertifikatskette vorweisen, so verwerfen die Nodes seine Router Advertisements.

Beschreibung

Bei SEND muss der Absender einer NDP Nachricht beweisen, dass er Eigentümer der entsprechenden Quelladresse ist. Zum Beweis, sendet er ein *CGA Option* genanntes Feld (siehe *[RFC3971, Kap 5]*) mit den entsprechenden Nachrichten mit. Dieses Feld enthält die in [RFC3972, Kap 3] beschriebenen *CGA Parameter*. Sie umfassen sowohl das Netzwerkpräfix als auch den zu Generierung der CGA genutzen öffentlichen RSA Schlüssel. Zusätzlich wird in [RFC3971, Kap 5] die *RSA Signature Option* eingeführt, welche es ermöglicht eine RSA Signatur beizufügen. Mittels dieser Signatur kann verifiziert werden, ob die Nachricht vom legitimen Inhaber der CGA stammt.

Um die Authentisitätsprüfung zu erzwingen, wird in [RFC3971, Kap 5] für alle Nodes die SEND verwenden vorgeschrieben, dass Neighbor Solicitation, Neighbor Advertisement, Router Advertisement und Redirect Nachrichten jeweils eine *RSA Signatur Option* enthalten müssen. Der RFC 3971 schreibt vor, dass die oben genannten NDP Nachrichten als unsicher zu betrachten und zu verwerfen sind, falls sie ohne eine RSA Signatur empfangen werden. Gleiches gilt, wenn die Verifizierung der CGA fehlschlägt oder die Signatur für die *CGA Parameter* invalide ist. Da nur der Eigentümer des privaten Schlüssels in der Lage ist eine Signatur für die CGA zu erstellen, kann so sichergestellt werden, dass es sich bei dem Absender einer NDP

Nachricht um den legitimen Eigentümer der Quelladresse handelt.

Die Signierung der NDP Nachrichten schützt zwar vor gefälschten Quelladressen, es wäre trotzdem noch möglich einen nicht autorisierten Router im Netz zu betreiben und so einen Traffic Hijacking Angriff (siehe 2.4.3) durchzuführen. Um dies zu verhindern, verwendet SEND einen zentralen Vertrauensanker, der den Nodes bekannt gemacht wird. Mittels Zertifikatsketten werden die Router von diesem Vertrauensanker dazu autorisiert Router Advertisements und Redirect Nachrichten zu versenden. Die Nodes können so die Authentizität der Router verifizieren.

Die kompletten Zertifikatsketten sind jedoch recht groß, sodass für sie ein spezieller Transportweg standardisiert wurde. Sie würden die Größe einzelner ICMPv6 Nachrichten sprengen und wenn sie immer mitgesendet werdeb würden, für unnötig viel Netzwerkverkehr sorgen. Deshalb führt SEND zur Verteilung von Zertifikatsketten mit der Certificate Path Solicitation und dem Certificate Path Advertisement (siehe [RFC3971, Kap 6]) neue ICMPv6 Nachrichten ein.

Mit der Certificate Path Solicitation kann ein Node von einem Router die Vertrauenskette anfordern. Darauf antwortet der Router mit einem Certificate Path Advertisement. Es beschreibt die Zertifikatskette vom Router zu einem dem Node bekannten Vertrauensanker. Jeder Schritt in der Kette bis zum Vertrauensanker wird dabei als eigene ICMPv6 Nachricht mit dem entsprechenden Zertifikat versendet. Die so erhaltene Zertifikatskette, kann der Node überprüfen, um sicherzustellen, dass der Router von dem Vertrauensanker autorisiert wurde.

Optional könnte sogar jeder Node eine Zertifikatskette zum Vertrauensanker erhalten, sodass jede für Neighbor Discovery verwendete IPv6 Adresse, immer zuerst durch den Vertrauensanker autorisiert sein muss. Dies stellt sich für die meisten Anwendungsfälle jedoch als unnötig und übermäßig aufwendig heraus, besonders weil der Aufwand für die Überprüfung der Zertifikatskette in diesem Fall viel öfter notwendig wäre. Außerdem würde durch die höhere Anzahl an Certificate Path Soliciations und Advertisements die Netzwerklast erhöht werden.

Nutzen

SEND erlaubt es kryptografisch, mittels CGA, sicherzustellen, dass kein Angreifer Neighbor Discovery Nachrichten mit einer gefälschten IPv6 Adresse versendet. Durch die Verwendung von CGA bleibt die Nutzung der IPv6 Adresse dem Eigentümer des

privaten Schlüssels vorbehalten. So kann das Netz effektiv gegen Angriffe gegen die Neighbor Discovery und die Neighbor Unreachability Detection abgesichert werden.

Die Autorisierung von Routern, mittels eines zentralen Vertrauensankers, verhindert das Versenden nicht autorisierter Router Advertisements. Die beschriebenen Angriffe auf die Router Discovery sind somit in einer SEND Umgebung nicht mehr möglich.

Ein weiterer Vorteil liegt darin, dass SEND diese Sicherheit unabhängig von der Sicherheit des Links und physikalischen Mediums, auf dem die Nachrichten transportiert werden, gewährt. Darin unterscheidet sich SEND somit von den Layer 2 und Hardwaremaßnahmen aus Abschnitt 4.1. Besonders in Situationen in denen die Sicherung des Links schwer zu realisieren ist, hat SEND somit Vorteile gegenüber anderen Schutzmaßnahmen.

Aktuelle Router von Cisco beherrschen bereits SEND. In dem Fall, dass solche eingesetzt werden, ist keine Veränderung an der Hardware notwendig. Es müsste nur die Konfiguration der Geräte entsprechend angepasst und Schlüssel für die Geräte durch den Vertrauensanker signiert werden.

Kosten

Der Einführung und der Einsatz von SEND zur Absicherung des Links sind jedoch auch mit einigen Nachteilen bzw. Kosten verbunden.

Da asymmetrische Kryptografie bei SEND eine maßgebliche Rolle spielt und für die einzelnen Neighbor Discovery Nachrichten angewendet werden muss, können diese aufwendigen kryptografischen Operationen selber zu einem Angriffsvektor werden. Wie in [RFC3971, Kap 9.3] beschrieben, können an einen Node viele Nachrichten (z.B. Neighbor Solicitations) gesendet werden, wobei er jeweils eine Verifikation der RSA Signatur durchführen muss. Dadurch können übermäßig viele Ressourcen in Anspruch genommen werden und es kann zu einem Denial of Service kommen. Gleiches gilt für den Versand von sehr langen Zertifikatsketten. Diese müssen vom Empfänger überprüft werden, wobei bei jedem Schritt die Anwendung aufwändiger asymmetrischer kryptografischer Operationen notwendig ist.

Der RFC empfiehlt eine Überwachung der verwendeten Ressourcen und wenn nötig, das selektive Verwerfen einzelner Pakete. Dies löst jedoch, genau wie die Überprüfung des Hashwerts, die ebenfalls empfohlen wird, das grundlegende Problem nicht. Dementsprechend muss davon ausgegangen werden, dass mit der Einführung von

SEND, auch neue Denial of Service Angriffsvektoren in das Netz eingebracht werden.

Eine Implementierung für einen Denial of Service Angriff auf SEND Umgebungen ist mit dem Tool *sendpees6* ebenfalls in der THC-IPv6 Suite enthalten.[2] Somit stellen derartige Angriffe ein praktisches Problem dar.

Außerdem ist der organisatorische Aufwand für die SEND Einführung nicht zu vernachlässigen. Neben der Installation eines SEND Clients auf allen Nodes, muss auch die sichere Verteilung des Vertrauensankers auf ebendiese gewährleistet werden. Dafür ist es entweder notwendig das IPv6-Netz zuerst ungesichert zu betreiben oder zum Verteilungszeitpunkt eine Verbindung über IPv4 herzustellen, über die die Verteilung stattfinden kann. Alternativ könnte das Zertifikat auch über ein externes Medium, wie einen USB Stick, auf die Endgeräte übertragen werden. Erst wenn die Verteilung sowie Konfiguration durchgeführt und die CGAs generiert wurden, kann der SEND-Betrieb aufgenommen werden. Es ist für die Einführung also ein nicht zu vernachlässigender Migrationsaufwand seitens der Netzwerk- und Systemadministratoren notwendig.

Für den Einsatz von SEND müssen alle Nodes des Links einen SEND verwenden. Dafür benötigen sie eine SEND Implementierung. Unter Linux stehen quell-offene SEND Implementierungen zur Verfügung, welche jedoch in der Praxis kaum verwendet werden. Eine offizielle Implementierung im Kernel ist nicht vorhanden. Für Windows stellt Microsoft keine eigene Implementierung bereit, dies scheint auch nicht in Planung zu sein. Es steht jedoch mit WinSEND[3] eine aktiv weiterentwickelte SEND Implementierung des Hasso Plattner Instituts bereit.

Gemein ist allen SEND Implementierungen, dass sie im User- und nicht im Kernel-Space implementiert sind, was die Performance negativ beeinflussen kann. Die empfangenen Neighbor Discovery Nachrichten müssen dabei jedes mal zuerst an den User-Space weitergereicht werden, um dort analyisiert und anschließend wieder in den Kernel-Space zurückgereicht zu werden. So kann durch einen von außen kontrollierten Vektor, die NDP Nachrichten, ein aufwendiger Kontext-Switch des Betriebssystems angestoßen werden. Ein Angreifer könnte dies unter Umständen als Denial of Service Angriffsvektor nutzen, indem er das Opfer mit NDP Nachrichten flutet. Auf jeden Fall würde bei einem hohen Aufkommen an NDP Nachrichten

[2] https://www.thc.org/thc-ipv6/- Abruf am 20.02.2014

[3] http://www.hpi.uni-potsdam.de/meinel/security_tech/ipv6_security/winsend.html - Abgerufen am 12.01.2014

das System mehr in Anspruch genommen werden als bei einer Implementierung im Kernel-Space.

Eine Implementierung im Kernel-Space bringt wiederum auch Nachteile mit sich. Für sie würden große Bibliotheken, unter anderem zum Verarbeiten der Zertifikate, im Kernel benötigt. Das würde den Quellcode des Kernel übermäßig aufgeblähen. Dies steht jedoch dem Ziel gegenüber die Codebase des Kernels so klein wie möglich zu halten, um seine Stabilität und Sicherheit zu gewährleisten. Somit stellt auch die Lösung im Kernel keine optimale Lösung dar.

In den Firmwares vieler Cisco Router ist eine SEND Implementierung mittlerweile standardmäßig enthalten, wenn die Leistungsfähigkeit der Router-Hardware dies zulässt. Für viel andere Geräte wie z.B. netzwerkfähige Drucker, Kameras usw. wird es jedoch in absehbarer Zeit keine SEND Implementierungen geben. Diese Geräte verfügen oft ohnehin über viel zu langsame Prozessoren, um die aufwendigen asymmetrischen kryptografischen Operationen durchzuführen. Dementsprechend bestünde auf vielen Netzwerkgeräten garkeine Möglichkeit zur Realisierung von SEND.

Auf einem Link müssen alle Nodes SEND verwenden oder keiner, ansonsten würde dies zu Inkonsistenzen in der Neighbor Discovery führen, welche Kommunikationsprobleme und die Einschränkung der Verügbarkeit des Netzes nach sich ziehen. Denn um einen wirksamen Schutz zu garantieren, dürfen Nodes die SEND verwenden lediglich signierte Neighbor Discovery Nachrichten akzeptieren. Die Folge dessen ist, dass alle Endgeräte, die nicht SEND unterstützen, in separate Netze verschoben werden müssen. Um dies umzusetzen wäre eine Umstrukturierung der internen Netzstruktur notwendig (siehe Abschnitt 4.4), die wiederum einen zusätzlichen Aufwand bedeutet. Besonders in sehr heterogenen Netzen können die verschiedensten Betriebssysteme und ihre jeweiligen SEND Implementierung oder der Mangel solcher, zu einem wichtigen Einflussfaktor für die Einführung von SEND werden.

SEND lässt sich wegen der aufgezeigten Defizite lediglich in homogenen Netzen, in denen sich alle Nodes unter einer zentralen administrativen Kontrolle befinden, sinnvoll einsetzen.

Neben den bereits genannten Nachteilen muss bei SEND außerdem angemerkt werden, dass die Schutzmaßnahme noch eher neu und durch seine krypografischen Designprobleme nicht sehr ausgereift scheint. Deshalb und weil unklar ist, ob sich SEND jemals durchsetzen wird, schrecken viele Hersteller bzw. Distributoren auch noch vor der Implementierung als Teil ihrer Betriebssysteme zurück.

4.3. Reaktive Maßnahmen

Als reaktive Maßnahmen werden solche bezeichnet, die einen Angriff nicht vorbeugen, sondern den Netzwerkverkehr überwachen, um Anomalien und Angriffe zu erkennen. Außerdem kann den erkannten Angriffen, im Rahmen der Intrusion Prevention, beispielsweise durch das Sperren der verwendeten Netzwerkports, entgegengewirkt werden. Auch die Korrektur unrechtmäßiger Änderungen durch Korrekturnachrichten stellt eine denkbare Reaktion dar.

Stellvertretend für eine ganze Reihe solcher Lösungen, wird hier mit NDPMon[4] die wohl bekannteste Monitoring Lösung für IPv6 Neighbor Discovery betrachtet. Alternativen die ebenfalls den Verkehr überwachen sind RAfixd[5] und RAMOND[6]. Diese sind jedoch weniger verbreitet sind und verfügen auch über weniger Funktionalitäten und Konfigurationsmöglichkeiten als NDPMon.

Beschreibung

Um NDPMon einzusetzen wird der Dienst auf einem System installiert, wobei Linux Distributionen, BSD und Mac OS unterstützt werden. Dieses System wird dann an den zu überwachenden Link angeschlossen, sodass an einer der Netzwerkschnittstellen der Neighbor Discovery Verkehr anliegt. Nach der Installation kann NDPMon auf Basis des normalen Verkehrs den Normalzustand lernen, um später Anomalien zu erkennen. Auch eine manuelle Konfiguration ist mittels einer XML Konfigurationsdatei möglich. So kann sicher gegangen werden, dass die wichtigsten Einstellungen wie Präfixe oder Router korrekt konfiguriert sind. Die Entwickler empfehlen dabei zuerst mittels der Lernfunktion eine Konfiguration zu erzeugen und diese dann manuell zu überprüfen und zu ergänzen.

Wird die Funktion zum automatischen Lernen der Konfiguration in einem bereits kompromittierten Netz genutzt, so kann eine vom Angreifer manipulierte Konfiguration gelernt werden. Dies hätte zur Folge, dass der NDPMon keine Ereignisse meldet, obwohl ein Angreifer in dem Netz aktiv ist. Es sollte also ein angriffsfreier Ausgangszustand gewährleistet werden, oder eine manuelle Konfiguration erfolgen.

[4] http://ndpmon.sourceforge.net/ - Abgerufen am 14.01.2014
[5] http://www.infoweapons.com/content/rafixd - Abgerufen am 14.01.2014
[6] http://ramond.sourceforge.net/ - Abgerufen am 14.01.2014

Dementsprechend ist bei der Konfiguration von NDPMon mit Vorsicht vorzugehen, um die Wirksamkeit der Schutzmaßnahme zu garantieren.

Im aktiven Betrieb untersucht NDPMon den Verkehr auf eine Reihe von Ungereimtheiten, wie z.B. falsche Router oder Präfixe. Wird eine Ungereimtheit erkannt, löst sie einen entsprechenden *Alert* aus, der von NDPMon aufgezeichnet wird. Zusätzlich gibt es die Möglichkeit für jeden *Alert* festzulegen, wie NDPMon darauf reagieren soll. Beispielsweise könnte NDPMon ein als schädlich erkanntes Router Advertisement automatisch wieder ungültig machen, indem ein weiteres Advertisement mit der Lifetime 0 erfolgt. Alternativ kann NDPMon auch nur rein passiv *Alerts* aufzeichnen oder den Administrator beispielsweise per Mail benachrichtigen, wenn *Alerts* auftreten.

Nutzen

Ein Vorteil dieser Maßnahme ist, dass sie auf jedem normalen Linux System in das Netz eingebracht werden kann. Existiert beispielsweise an dem Link schon ein Linux Server, so kann NDPMon einfach als weiterer Dienst eingerichtet werden. Die komplette Software ist quell-offen und frei, sodass auch beim großflächigen Einsatz keine Kosten dafür anfallen. Wichtig ist auch, dass die Funktion der Netzwerkinfrastruktur nicht direkt durch das Einbringen von NDPMon beeinflusst wird, da das Gerät, außer bei der Korrektur erkannter Angriffe, keinen Einfluss auf den Verkehr nimmt. So ist die Integration in die Netze ohne Downtime möglich. Durch die Möglichkeit auf Basis des normalen Verkehrs die Umgebungsparameter zu lernen, kann der Einrichtungsaufwand reduziert werden, ohne den Administratoren die Möglichkeiten manueller Änderungen zu nehmen.

Durch die detaillierten Logs über die NDP Nachrichten und Ereignisse können später die Vorkommnisse untersucht und unter Umständen die Schuldfrage bei Angriffen geklärt werden. In den meisten größeren Unternehmensnetzen findet sich eine Infrasturktur zur zentralen Aggregierung und Auswertung von Logdaten. Da NDPMon das standardisierte Syslog Protokoll [RFC5424] für die Aufzeichnung verwendet, können die NDPMon-Logs einfach aggregiert und zentral auf Vorkommnissen untersucht werden. Alternativ zu Lösungen die auf der Analyse der Logdateien basieren, kann auch Monitoring mittels Nagios eingesetzt werden, um Rückmeldungen über Alerts zentral zu sammeln, siehe Abschnitt 6.4. So kann die zentrale Überwachung der Vorkommnisse sehr komfortabel durchgeführt werden.

NDPMon kann sowohl Manipulationen an Router Discovery, wie z.B. Traffic Hijacking Angriffe, als auch an der Neighbor Discovery erkennen. Dabei werden zum Beispiel sich verändernde MAC-Adressen in Kombination mit der gleichen IPv6 Adresse oder veränderte Netzwerkparameter erkannt. Durch die Gegenmaßnahmen und Benachrichtigung der Administratoren, kann NDPMon effektiv eine wesentliche Rolle beim Schutz des Links spielen.

Kosten

Befinden sich noch keine geeigneten Linux Systeme im Netz, oder sollen separate Systeme genutzt werden, treten Anschaffungs- und Unterhaltskosten für diese neuen Server auf. Eine Möglichkeit wären hier zentral aufgestellte Server mit mehreren Netzwerkschnittstellen, die die Überwachungsaufgabe für mehrere Netze gleichzeitig erfüllen können. Dieses System sollte jedoch gut gehärtet und ständig aktualisiert werden, um zu verhindern, dass es kompromittiert und von Angreifern genutzt wird, um in andere Netze vorzudringen. Aufgrund des so entstehenden Aufwands ist es eher zu empfehlen für jeden Link ein separates Überwachungssystem einzusetzen.

Beim Einsatz einer Überwachungslösung wie NDPMon muss sichergestellt werden, dass die Administratoren den gemeldeten Ereignissen auch nachgehen. Ansonsten wäre die Maßnahme bestenfalls unwirksam oder gar kontraproduktiv, da beispielsweise durch False-Positives ausgelöste Gegenmaßnahmen die Verfügbarkeit des Netzes beeinflussen könnten. Dementsprechend ist mit dem Betrieb ein regelmäßiger personeller Aufwand verbunden. Bei Änderungen an der Netzwerkkonfiguration muss auch gleichzeitig die Konfiguration des NDPMon angepasst werden. In einem solchen Fall würde das konfigurierte Profil nicht mit den neuen Einstellungen übereinstimmen. Dies könnte zu Fehlfunktionen oder Störungen führen. Der Prozess der Anpassung sollte im Rahmen der Change Management Prozesse abgebildet werden, sodass immer ein sicherer Zustand garantiert werden kann.

Als Nachteil von NDPMon ist anzumerken, dass die Entwicklung scheinbar aktuell nicht aktiv weiter vorangetrieben wird. Die letzte veröffentlichte Version 2.1 stammt aus dem Jahr 2012. Zwar sind alle Kernfunktionen bereits implementiert, zusätzliche Möglichkeiten wie ein Webinterface und verteilte Datensammlung sind jedoch noch experimentell und nicht für den produktiven Betrieb geeignet. Es bleibt also zu hoffen, dass im Zuge der steigenden Verbreitung von IPv6 auch dieses Projekt wieder aktiv weiterentwickelt wird.

4.4. Architektonische Maßnahmen

Mit architektonischen Maßnahmen ist die Restrukturierung bestehender Netze gemeint. Die Einführung von IPv6 bietet eine gute Möglichkeit, die bestehende Netzwerkarchitektur, welche über Jahre gewachsen ist, in eine logische und optimierte Struktur zu überführen. Zudem bietet IPv6 auch bei der Nutzung von global eindeutigen Adressen. Mit einem */56* oder einem */48* Präfix existiert in IPv6 Netzen genug Spielraum um viele kleine Netze zu betreiben.

Bei der Restrukturierung wird versucht, die Systeme nach verschiedenen Faktoren in Gruppen einzuteilen. Ein wichtiges Kriterium ist ihr Typ. Handelt es sich um einen intern bzw. extern erreichbaren Server oder um eine Workstation? Dementsprechend kann es sinnvoll sein diese in jeweils eigene Netze einzuordnen. Außerdem muss die Zugehörigkeit zur Geschäftseinheit und die Klassifikation der verarbeiteten Daten berücksichtigt werden, denn daraus ergeben sich auch die zu erwartenden Verkehrsflüsse.

Von einem Switch mit ensprechender Funktion können mittels VLANs mehrere Netze angeboten werden. Abhängig von dem Port (bzw. anderen Faktoren) kann den angeschlossenen Nodes das zu verwendene VLAN zugewiesen werden. Die Switches und Router werden über sogenannte Trunk Ports miteinander verbunden. So kann an vielen Stellen auf zusätzliche Hardware verzichtet werden. In vielen Netzen werden ohnehin schon VLANs eingesetzt, um beispielsweise Voice over IP Systeme von den restlichen Endgeräten zu trennen. Werden VLANs eingesetzt, so ist die Umstrukturierung oft zu großen Teilen mittels Konfigurationsanpassungen möglich (siehe [Boek2012, Kap 5.1.2, S. 157ff]).

Nutzen

Durch die Maßnahme kann die Angriffsfläche stark reduziert werden, da die Anzahl der Systeme, die sich auf dem gleichen Link befinden wie der Angreifer, stark sinkt. Außerdem sind bei korrekter Umsetzung sensiblere Systeme, wie wichtige Server, nicht angreifbar, sondern nur Systeme die in Typ und Wichtigkeit dem Ausgangssystem des Angreifers ähneln. Das schränkt die Auswirkungen und den Nutzen erfolgreicher Angriffe für den Angreifer weiter ein.

Die Schaffung einer neuen Struktur, bildet auch die Grundlage für ein in Zukunft

strukturiertes und weniger komplexes Netz. Dadurch kann dessen zukünftiger Wartungsaufwand reduziert und die Verständlichkeit für Administratoren erhöht werden. Gleichzeitig sinkt die Grundlast durch IPv6 Multicast Verkehr für NDP, da dieser nur in den kleineren Netzen jeweils intern stattfindet, also nicht den ersten Router überwindet.

Kosten

Unter Umständen kann die Restrukturierung bestehender und historisch gewachsener Firmennetzwerke mit einem hohen organisatorischen Aufwand verbunden sein. Denn dabei muss jedes Endsystem erfasst und entsprechend der definierten Kriterien einem Netz zugeordnet werden. Außerdem müssen die Router und Firewalls zwischen den Netzen so konfiguriert werden, dass die normalen Arbeitsabläufe problemlos weiter stattfinden können. Andernfalls kann es leicht dazu kommen, dass die Funktionsfähigkeit von Teilen des Netzes eingeschränkt und so Arbeitsprozesse behindert werden.

Da die Zahl der Links steigt und diese jeweils mittels eines Routers angebunden werden müssen, kann es dazu kommen, dass weitere Router für die neu entstandenen Links angeschafft werden müssen. Außerdem kann es, abhängig von den bisher eingesetzten Switches, notwendig werden, diese durch solche mit VLAN-Funktionalität auszutauschen.

5. Bewertung

In Kapitel 4 wurden verschiedene möglicher Schutzmaßnahmen gegen die Angriffe aus Kapitel 3 vorgestellt. Bei genauerer Betrachtung wird klar, dass keine dieser Maßnahmen alleine einen perfekten Schutz gegen alle Angriffe bietet. Dabei stellt sich heraus, dass nicht jede Maßnahme für jede Umgebung geeignet oder sinnvoll ist. Deshalb wird in diesem Kapitel versucht, die Maßnahmen einzuordnen und konkrete Empfehlungen für deren Anwendung in der Praxis zu geben.

5.1. Maßnahmenbewertungen

Jede der beschriebenen Maßnahmen bringt gewisse Vor- und Nachteile mit sich. In diesem Abschnitt werden die bisher betrachteten Maßnahmen unter verschiedenen Aspekten bewertet und miteinander verglichen.

5.1.1. Layer 2 und Hardware

Vorteile Die durch die Netzwerkhardware umgesetzen Schutzmaßnahmen (siehe Abschnitt 4.1) bringen alle den Vorteil mit sich, dass sie für die Endgeräte transparent in die Netze integriert werden können.

Nachteile Jedoch ist eine Unterstützung durch die Switches notwendig. Wenn nicht bereits Switches mit den erforderlichen Funktionen eingesetzt werden, müssen sie gegen solche ausgetauscht werden. Abhängig davon wieviele Geräte neu beschafft werden müssen, kann dies einen hohen finanziellen Aufwand nach sich ziehen, insbesondere da die Maßnahmen meist nur von vergleichsweise teuren Geräten unterstützt werden.

Zudem ist der Einsatz der Maßnahme meistens nur sinnvoll, wenn sie durch alle Switches des Links angewendet wird. Andernfalls kann der Sicherheitsgewinn stark

reduziert werden, da Angreifer die ungeschützten Switches für ihre Angriffe nutzen könnten. Selbiges gilt für die physikalische Sicherheit der Netzwerkhardware. Kann ein Angreifer mit geringem Aufwand physikalischen Zugang zu einem Trunk Port bzw. Trusted Port erhalten, so sind alle Schutzmaßnahmen auf Ebene der Netzwerkinfrastruktur wirkungslos. Eine flächendeckende Einführung ist somit unabdingbar zur Gewährleistung der Wirksamkeit der eingesetzten Maßnahme.

RA-Guard

Vorteile Der RA-Guard ist die heute am weitesten verbreitete Schutzmaßnahme auf der Ebene der Netzwerkhardware. Er kann jedoch nur vor Angriffen mittels gefälschten und manipulierten Router Advertisements schützen. Dennoch ist es auch heute schon in verhältnismäßig vielen Switches der großen Hersteller zu finden.

Nachteile Der RA-Guard lässt sich, wie in Abschnitt 4.1.1 beschrieben, leicht durch gezielte Fragmentierung der IP-Pakete umgehen. Das in 4.1.4 beschriebene Fragmentierungsverbot für Neighbor Discovery Nachrichten adressiert genau diese Schwachstelle. Dennoch muss bedacht werden, dass die Änderung des RFCs erst in den IPv6 Implementierungen umgesetzt werden muss. Es kann dabei einige Zeit vergehen, bis die entsprechenden Updates die verschiedenen Systeme erreichen. Besonders eingebettete Systeme werden in den meisten Fällen keine entsprechende Updates erhalten. Es handelt sich bei dem Fragmentierungsverbot also nur um eine langfristige Lösung des Problems. In absehbarer Zeit wird sich der Schutz des RA-Guard dementsprechend noch oft mittels Fragmentierung umgehen lassen.

Kurzfristig kann zumindest ein Teil der Systeme durch die Konfiguration der Paketfilter auf den Endgeräten geschützt werden. Dies bietet wiederum keinen Schutz für eingebettete Systeme, da diese in der Regel über keine derartig konfigurierbaren Paketfilter verfügen. Außerdem müssen die entsprechenden Regelsätze auf alle Endgeräte des Links verteilt werden. Dennoch können so, mit einfachen Mitteln, Angriffe auf viele der eingesetzten Endgeräte verhindert werden.

Durch die RFC-Änderung [RFC7112], die beschreibt, dass der ULP Header im ersten Fragment enthalten sein muss, können Switches in Zukunft fragmentierte NDP Nachrichten verwerfen. Würde dies umgesetzt, so könnte der RA-Guard nicht mehr durch Fragmentierung umgangen werden. Auf diese Weise würden alle Endgeräte vor fragmentierten NDP Nachrichten geschützt.

FCFS-SAVI

FCFS-SAVI ergänzt die Schutzmaßnahmen, um einen Schutz der Neighbor Discovery, vor allem vor Neighbor Cache Poisoning. Jedoch ist der Standard noch sehr neu und es existieren noch keine praktischen Implementierungen. Dennoch wurde hier ein Standard geschaffen, der die Hardware-Schutzmaßnahmen in Zukunft herstellerunabhängig und sinnvoll ergänzen wird.

Cisco IPv6 First Hop Security

Wie in 4.1.3 beschrieben, verfügt Cisco über zahlreiche eigene Schutzmaßnahmen, die auf jeden der Angriffe eine Antwort bieten. Diese Palette besteht aus Maßnahmen wie dem RA-Guard und einer FCFS-SAVI ähnlichen Implementierung, dem IPv6 Source Guard. Hier ist jedoch zu bedenken, dass zwar eine umfangreiche Palette an Maßnahmen geliefert wird, jedoch eine starke Bindung an den Hersteller Cisco eingegangen wird. Zudem sind die Sicherheitsfunktionen zumeist nur in hochpreisigen Switches überhaupt enthalten, sodass hohe Kosten bei Neuanschaffungen auftreten können.

Einordnung

Insgesamt sind die Schutzmaßnahmen auf Ebene der Netzwerkinfrastruktur noch nicht sehr weit verbreitet. Sie sind in vielen Fällen auch noch angreifbar oder noch nicht ausgereift. Außerdem ist der notwendige Austausch ganzer Teile der Switching-Infrastruktur mit einem beträchtlichem Aufwand, sowohl personell als auch finanziell, verbunden.

5.1.2. Kryptografische Schutzmaßnahmen

Eine Alternative zur Implementierung in Netzwerkhardware bieten die kryptografischen Lösungen. Sie setzen auf dem Endgerät an und erfordern dort somit eine Implementierung entsprechender Protokolle sowie eine dazugehörige Konfiguration.

IPsec

IPsec könnte theoretisch den NDP Verkehr absichern [RFC4861]. Viele der IPv6 Implementierungen verfügen zwar über eine IPsec Unterstützung, dennoch stellt die Schlüsselverteilung ein großes Problem dar. Eine manuelle Schlüsselverteilung ist in praktischen Szenarien kaum denkbar und mit hohem Wartungsaufwand verbunden. Aktuell erscheint IPsec somit ungeeignet für den Einsatz als Schutzmaßnahme für NDP.

SEND

Vorteile SEcure Neighbor Discovery führt ein komplett neues kryptografisches Protokoll für sichere Neighbor Discovery ein. Dies ist im Gegensatz zu den Schutzmaßnahmen auf Schicht 2 nicht auf die Sicherheit des Links angewiesen.

Nachteile Ein großes Problem stellt hier jedoch dar, dass alle Endgeräte und auch Router in einem Netz SEND unterstützen müssen. Problematisch wird dies insbesondere dadurch, dass für viele Plattformen keine SEND Implementierungen existieren. Dies führt dazu, dass ein Teil der Systeme in andere Netze verschoben werden muss, um einen stabilen Netzwerkbetrieb zu gewährleisten. Dies bringt wiederum zusätzlichen Aufwand mit sich. Auch für die Systeme, für die eine SEND Implementierung vorliegt, fällt jeweils personeller Aufwand für die Installation und Einrichtung von SEND an.

Um die Sicherheit der Router Discovery mittels SEND zu gewährleisten, wird zusätzlich eine Public-Key Infrastruktur benötigt, um einen Vertrauensanker zur Verfügung zu stellen. Mit diesem Anker werden die Router zum Versand von Router Advertisements autorisiert. Um die Autorisierung zu überprüfen, ist eine sichere Verteilung der Zertifikate des Vertrauensankers notwendig.

Außerdem bringt SEND durch das nicht durchdachte kryptografische Protokoll und die exzessive Nutzung asymmetrischer Kryptografie neue Denial of Service Angriffsvektoren mit sich. Dies stellt ein Designproblem von SEND dar, welches bei allen Implementierungen vorliegt. Es eröffnet einem Angreifer die Möglichkeit zum DOS Angriff auf beliebige Systeme. Unter Beachtung des hohen Aufwands für die Einführung und des Entstehens des DOS Angriffsvektors ist es fraglich, ob die Einführung von SEND die Lösung der Wahl darstellt.

5.1.3. Reaktive Maßnahmen

Vorteile Eine Alternative oder Ergänzung, zu den bisher genannten Maßnahmen, können die in Abschnitt 4.3 beschriebenen reaktiven Maßnahmen darstellen. Sie lassen sich einfach in ein Netz einbringen, ohne die bestehende Infrastruktur zu beeinflussen. An Endgeräte oder Netzwerkhardware werden bei reaktiven Maßnahmen keine Anforderungen gestellt, was die Integration in jede Umgebung denkbar macht.

Es ist lediglich ein Linux Server notwendig, der permanent mit dem entsprechenden Link verbunden ist, um den NDP Verkehr zu überwachen. Unter Umständen muss dabei für jeden Link ein neuer Server aufgestellt werden. Die damit verbundenen Kosten müssen somit in die Betrachtung mit einbezogen werden. Da der Server jedoch keine besonderen Anforderungen erfüllen muss, kommen auch günstige Linux-Systeme in Frage. Dementsprechend sind die Kosten für die Überwachungssysteme vergleichsweise gering einzustufen.

Bei der Einführung offenbart sich ein weiterer Vorteil, denn die reaktive Maßnahme NDPMon, kann schrittweise in das Netz integriert werden. Im ersten Schritt kann der aktuelle Zustand der Netzwerkkonfiguration gelernt und die Konfiguration des Dienstes entsprechend angepasst werden. Danach kann in einen Überwachungsbetrieb übergegangen werden, in dem keine aktiven Eingriffe in das Netz erfolgen, sondern nur Meldungen an den Administrator. Funktioniert die Maßnahme in diesem Modus ohne Probleme, so können schließlich Gegenmaßnahmen aktiviert und das volle Potential der Maßnahme ausgeschöpft werden. Durch dieses schrittweise Vorgehen können, durch die Einführung der neuen Maßnahme, auftretende Störungen des Netzes verhindert und die Administratoren langsam an die neue Schutzmaßnahme herangeführt werden.

Nachteile Wie bei allen Intrusion Detection Lösungen sollten die Meldungen des Überwachungsdienstes auch analysiert werden. Ansonsten kann die Wirksamkeit der Maßnahme eingeschränkt sein.

Reaktive Schutzmaßnahmen verhindern nicht proaktiv das Ausnutzen einer Schwachstelle. Der potentielle Schaden wird jedoch durch automatische Korrekturen auf ein geringeres Maß reduziert. Dennoch existiert noch immer ein Restrisiko, dass ein Node beispielsweise einen unautorisierten Router verwenden, noch bevor ihn die Korrekturnachricht des NDPMon erreicht. Dieses Restrisiko ist jedoch relativ gering, sodass es in den meisten Fällen akzeptiert werden kann.

5.1.4. Architektonische Maßnahmen

Nachteile Bei der Restrukturierung kann der Planungs- und Umsetzungsaufwand, besonders bei großen und gewachsenen Netzen, schnell sehr hoch werden. Insbesondere wenn auch Teile der Netzwerkhardware oder Verkabelung ausgetauscht oder ergänzt werden müssen, führt dies zu unverhältnismäßig hohen Kosten. Einen weiteren Kostenfaktor ist, dass während der Migration zeitweise Störungen der Verfügbarkeit auftreten können. So können Arbeitsabläufe zeitweise beeinflusst oder unterbrochen werden. So entstehende Kosten sollten in die Überlegungen einbezogen werden.

Wegen des teilweise hohen Aufwands für die Restrukturierung, erscheint diese in vielen Umgebungen alleine als Schutzmaßnahme eher nicht sinnvoll. Im Rahmen allgemeiner Restrukturierungsmaßnahmen lässt sich die Netzwerksicherheit aber leicht berücksichtigen.

Vorteile Durch die Restrukturierung der Netze, die ohnehin in vielen gewachsenen Netzen, im Rahmen der Einführung von IPv6 sinnvoll ist, können Systeme verschiedener Wichtigkeit getrennt werden. Die Zahl möglicher Ziele und die Auswirkungen von erfolgreichen Angriffen können, durch die Verwendung verschiedener Netze, stark gemindert werden.

Außerdem können in den kleineren Netzen schneller weitere Sicherheitsmaßnahmen, wie beispielsweise solche von Switches, eingeführt werden. Davon betroffen sind insbesondere Maßnahmen, die gleichzeitig für alle Switches oder Endgeräte auf einem Link eingeführt werden müssen. Bei kleineren Netzen kann Netz für Netz die neue Sicherheitsmaßnahme eingeführt werden. Außerdem ist es somit auch möglich zu entscheiden, welche Netze einen besonderen Schutzbedarf besitzen und so zu entscheiden wo bestimmte Maßnahmen überhaupt sinnvoll sind. Dies kann den Aufwand zur Absicherung der Netze mitunter stark reduzieren und so zu einer effizienteren Umsetzung führen.

Wird allgemein an der Restrukturierung im Rahmen der Einführung von IPv6 gearbeitet, so können Sicherheitsaspekte leicht einbezogen werden. Dadurch kann ein relevanter Sicherheitsgewinn entstehen.

Architektonische Maßnahmen bieten sich unterstützend zu jeder der genannten Maßnahmen an und sind auch aus Sicht der Netzwerkadministration in den meisten Fällen allgemein sinnvoll.

5.2. Bewertungsmatrix

Um einen Überblick über die Maßnahmen, ihre Stärken und Schwächen und die mit ihnen verbundenen Kosten zu erleichtern, werden diese Informationen so in einer Tabelle gegenübergestellt, sodass Vor- und Nachteile leicht sichtbar werden. Grundsätzlich kann bei jeder Eigenschaft entweder ein guter (+), mittlerer (~) oder schlechter (-) Wert erzielt werden. Es wurde also ein sehr reduziertes Bewertungsschema verwendet. Nachfolgend werden die aufgetragenen Bewertungskriterien beschrieben und definiert wie die Klassifizierung jeweils durchgeführt wurde.

Schutz gegen Angriffe

Zuerst betrachtet wurde, welche der in Kapitel 3 dargestellten Angriffe überhaupt mit einer bestimmten Maßnahme verhindert werden können. So kann leicht erkannt werden, ob noch zusätzliche Maßnahmen notwendig wären, um das Schutzprofil zu ergänzen. Für jeden Angriffsvektor wird bewertet, wie gut der Schutz gegen ihn ist.

gut Maßnahme verhinder effektiv diese Art von Angriffen.

mittel Grundsätzlicher Schutz gegen derartige Angriffe ist gegeben, jedoch unter bestimmten Rahmenbedingungen unwirksam.

schlecht Keinerlei praktisch relevanter Schutz gegeben.

Umgehbarkeit

Um die Wirksamkeit einer Maßnahme einzuschätzen ist es zudem noch relevant zu betrachten, inwiefern die Maßnahme durch einen Angreifer umgangen werden kann und wie hoch der Aufwand dafür ist.

schlecht Die Maßnahme lässt sich leicht umgehen (z.B. RA-Guard in der Standardkonfiguration).

mittel Ein Umgehen der Maßnahme ist mit hohem Aufwand möglich, z.B. durch physikalischen Zugriff auf bestimmte Ports eines Switches.

gut Der Aufwand ist noch höher, z.B. der Angriff nur durch Kompromittierung der Endgeräte bzw. Router möglich. Oder das Umgehen ist praktisch garnicht möglicht.

Anforderungen an Hardware

Um den Aufwand der Einführung einer Maßnahme zu bestimmen, wird zunächst betrachtet welche Anforderungen an die Hardware bzw. Plattformen gestellt werden. Dabei werden Switch, Router und Endgeräte unterschieden.

gut Es existieren keinerlei Anforderungen, die Maßnahme ist gegenüber diesen Geräten transparent.

mittel Die Maßnahme erfordert zwar spezielle Funktionalitäten, diese sind jedoch in relativ günstigen Hardwaremodellen verfügbar, bzw. es sind für viele Plattformen Implementierungen vorhanden.

schlecht Die Maßnahme ist nur auf High-End Geräten zu finden bzw. auf nur wenigen Plattformen ist eine gute Unterstützung gegeben.

Aufwand für Einführung

Anschließend wird betrachtet wie hoch die Kosten zur Einführung der Maßnahme in einem bestehenden Netz sind.

gut Es müssen keine oder nur wenige Geräte getauscht bzw. neu angeschlossen werden und es tritt nur geringer initialer Konfigurationsaufwand auf.

mittel Teile der Hardware müssen zwar ausgetauscht werden, jedoch nur durch gängige Hardware des mittleren Preissegments.

schlecht Es müssen große Teile der Netzwerkhardware durch spezielle teuere Hardware ausgetauscht werden, oder ist eine sehr aufwendige manuelle Konfiguration jedes Geräts nötig.

Kosten für den Betrieb

Zusätzlich werden noch die Betriebskosten betrachtet, die nach der Einführung regelmäßig anfallen.

gut Die Schutzmaßnahme funktioniert auch wirksam ohne, dass ein Administrator regelmäßig Aufwand für ihren Betrieb aufwenden muss effektiv.

mittel Es ist beispielsweise eine regelmäßige Sichtung der Warnungen und Meldungen notwendig, um einen wirksamen Schutz zu garantieren.

schlecht Um die Funktionsfähigkeit des Netzes zu garantieren, ist mit substantiellem administrativem Aufwand in regelmäßigen Abständen zu rechnen.

Entwicklungsstand

Der Entwicklungsstand beschreibt wie weit die Entwicklung der Schutzmaßnahme fortgeschritten ist.

gut Die Entwicklung sehr weit fortgeschritten. Die Schutzmaßnahme ist in der Praxis anwendbar und erprobt.

mittel Die Grundlagen und Standards für die Maßnahme sind geschaffen. Es existieren jedoch noch Defizite bei ihrer praktischen Realisierung.

schlecht Die Umsetzung dieses Ansatzes ist in der Praxis noch bei weitem nicht erreicht. Eine solche Maßnahme ist höchstens zu Testzwecken, aber nicht für den produktiven Betrieb geeignet.

Verbreitung

Abschließend wird betrachtet wie verbreitet die Maßnahme ist, bzw. wie gut die Verfügbarkeit von Hardware mit den ensprechenden Maßnahmen ist.

gut Die Implementierung ist für freie Plattformen und z.B. als quelloffene Software wie NDPMon verfügbar. Oder die Maßnahme ist beispielsweise in Form eines Features des Switches, schon in vielen Geräten anzutreffen, sodass eine gewisse Auswahl und Verbreitung besteht.

mittel Es bestehen wie bei SEND noch Defizite bei der Verbreitung, weil beispielsweise für viele Plattformen noch keine Implementierung existiert. Für die wichtigsten Plattformen existiert jedoch grundsätzlich eine Implementierung.

schlecht Es gibt noch kaum oder garkeine praktische Realisierungen bzw. nur sehr wenige spezielle Geräte, einzelner Hersteller, die überhaupt die Maßnahme umsetzen.

Maßnahme:	RA-Guard	FCFS-SAVI	Cisco First-Hop[1]	IPsec	SEND	NDPMon
Schutz gegen:						
Neighbor Cache Poisoning	-	+	+	+	+	~
NUD[2] DOS	-	+	+	+	+	+
DAD[3] DOS	-	+	+	+	+	+
RA[4] Spoofing	+	-	+	+	+	+
Performance Degrading	+	-	+	+	+	+
DHCPv6	-	-	+	-	-	-
Umgehbarkeit	**schlecht (mittel)**[5]	**mittel**	**mittel**	**gut**	**gut**	**mittel**
Anforderungen an Switches	~	-	-	+	+	+
Anforderungen an Router	+	+	+	~	~	+
Anforderungen an Endgeräte	+ (~) [5]	+	+	~	~	+
Kosten für Einführung	~	-	-	-[6]	-	+
Kosten für Betrieb	+	+	+	-[6]	~	~
Entwicklungsstand	+	~	+	-[7]	~	+
Verbreitung/Verfügbarkeit	+	-	-	-[7]	~	+

Tabelle 5.1.: Übersicht: Maßnahmen

Betrachtung architektonischer Maßnahmen

Bei der tabellarischen Betrachtung der Maßnahmen wurden die architektonische Maßnahmen, die in Abschnitt 4.4 beschrieben sind, nicht separat aufgeführt. Sie verhindern prinzipbedingt keine Art des Angriffs grundsätzlich. Durch sie werden jedoch die möglichen Ziele, die angreifbar sind, stark reduziert. So lassen sich die Möglichkeiten eines Angreifers stark einschränken. Grundsätzlich sind sie jedoch wie in Abschnitt 4.4 beschrieben zur Ergänzung aller anderen Maßnahmen geeignet.

5.3. Empfehlungen

Als konkrete Empfehlung für die Einführung zusätzlicher Sicherheitsmaßnahmen in bestehende Umgebungen sind vor allem reaktive Maßnahmen wie NDPMon zu nennen. Sie lassen sich einfach in bestehende Netze integrieren und sind nur mit relativ geringen Kosten für die Einführung verbunden. Dennoch verhindern sie den meisten Schaden durch Angriffe mittels NDP. Auch als Übergangslösung sind reaktive Lösungen sehr gut geeignet, da sie sich später ohne großen Aufwand aus dem Netz entfernen lassen.

Steht ohnehin die Umstrukturierung der Netze an, so kann diese, wenn sie mit Blick auf die Sicherheit durchgeführt wird, einen Sicherheitsgewinn bedeuten und ist somit empfehlenswert. Als eigene Maßnahme zur Erhöhung der Sicherheit, macht die Umstrukturierung nur Sinn, wenn die Kosten im konkreten Fall nicht zu hoch sind. Außerdem werden durch die Umstrukturierung keine Angriffe verhindert, sondern nur die Ziele möglicher Angriffe eingeschränkt und so die Auswirkungen reduziert.

In Zukunft wird die Zahl der Switches mit IPv6 Sicherheitsfunktionen immer weiter steigen. Wenn neue Geräte angeschafft werden, ist es eine Überlegung wert, solche mit entsprechenden Funktionen zu kaufen. Dies müsste jedoch flächendeckend durchgeführt werden. Im Laufe der Zeit wird sich auch das Fragmentierungsverbot

[1] Cisco IPv6 First-Hop Security Features
[2] Neighbor Unreachability Detection
[3] Duplicate Address Detection
[4] Router Advertisement
[5] Wenn Fragmentierung mittels Maßnahmen auf Endgeräten verhindert wird, z.B. Firewalls
[6] Bei manueller Schlüsselverteilung, automatisiert wegen IKE Problematik nicht möglich. Wenn das Problem gelöst würde, würden die Kosten drastisch sinken.
[7] Keine praktische Umsetzung bzw. Anwendung absehbar

für Neighbor Discovery Nachrichten, immer weiter durchsetzen, sodass Fragmentierungsangriffe gegen viele Systeme schwieriger werden. Die RA-Guard Implementierungen werden jeweils so aktualisiert werden, dass sie Nachrichten die nicht den ULP Header im ersten Fragment enthalten verwerfen. Insgesamt ist damit zu rechnen, dass deshalb das Umgehen des RA-Guard mittels Fragmentierung langfristig nicht mehr möglich sein wird. Es kann davon ausgegangen werden, dass in einigen Jahren auch Sicherheitsfunktionen auf Netzwerkinfrastrukturebene kostengünstig und effektiv einsetzbar sein werden. Dennoch erfordern diese immer eine entsprechende Ausstattung der Switches.

Die kryptografischen Sicherheitsmaßnahmen können, besonders aufgrund grundlegender Fehler und fehlender Implementierungen, nicht überzeugen. Von ihrem Einsatz, insbesondere bei SEND, kann aktuell nur abgeraten werden, da neue Angriffspotentiale entstehen. Außerdem ist die Verbreitung auf den Endsystemen noch nicht weit genug fortgeschritten, sodass sich eine Migration in bestehenden Netzen schwierig gestalten kann.

6. Einsatzbeispiel für NDPMon

Bei der Bewertung wurde festgestellt, dass sich reaktive Maßnahmen wie NDPMon sehr gut zur zusätzlichen Absicherung von IPv6 Netzwerken eignen. Gleichzeitig wurde in Abschnitt 4.3 festgestellt, dass ein immer verfügbares System für jeden Link benötigt wird. Um bestehende produktive Systeme nicht zusätzlich damit zu belasten und eine universell einsetzbare sowie kosteneffiziente Lösung für alle Links eines Netzwerks zu schaffen, wird nachfolgend eine Plattform auf Grundlage des ARM-Systems Raspberry Pi vorgestellt.

6.1. Der Raspberry Pi

Bei dem Raspberry Pi[1] handelt es sich um einen Einplatinencomputer, der die handliche Größe einer Kreditkarte besitzt. Er basiert auf einem ARM11 Prozessors mit 700 MHz Taktung. Nachfolgend kommt das Modell B des Raspberry Pi zum Einsatz, welches derzeit für ca. 35€ im Handel angeboten wird. Es verfügt über 512 MB Arbeitsspeicher, zwei USB 2.0 Ports, HDMI, sowie einen SD-Kartenleser und einen 100 MBit Ethernet-Port. Die Stromversorgung des Raspberry Pi ist über einen USB Port oder über ein optionales Netzteil möglich.

Mit diesen Merkmalen bietet der Raspberry Pi eine gute Grundlage für den Betrieb eines Linux Systems. Außerdem ist der Raspberry Pi eine weit verbreitete und einheitliche Plattform, die über viele Quellen bezogen werden kann, sodass die Beschaffung kein Problem darstellt. Ebenfalls sind eine Vielzahl passender Gehäuse und Zubehör verfügbar, eine Anpassung an die Bedürfnisse ist somit einfach möglich.

[1] http://www.raspberrypi.org/ - Abgerufen am 20.01.2014

6.2. Das Betriebssystem

Als Betriebssystem kommt hier Raspbian zum Einsatz. Dabei handelt es sich um eine auf die Plattform angepasste Version der beliebten und weit verbreiteten Debian Linux Distribution. Raspian wurde wegen seiner großen Entwicklergemeinschaft und weiten Verbreitung gewählt. Die meisten Administratoren sind schon mit Linux Systemen wie Debian oder Ubuntu vertraut, was die Einrichtung und Wartung entsprechender Systeme in Zukunft vereinfachen sollte. Durch die Verwendung von Debian und die Funktionalität für automatische Updates kann zudem gewährleistet werden, dass das Überwachungssystem immer auf dem aktuellen Stand ist.

6.3. NDPMon Installation

Da NDPMon in aktueller Version nicht als Paket für Debian vorliegt, sollte das Programm auf Basis der vorliegenden Quellcodes neu kompiliert werden. Dafür wird sowohl auf die Installationsanleitung auf der Website der Entwickler von NDPMon,[2] als auch auf die Anleitung „NDPMon running in Raspberry Pi“ verwiesen.[3] Dort werden die Schritte und entsprechende Konfigurationsparameter angegeben. Es empfiehlt sich nach aktuellem Entwicklungsstand von NDPMon jedoch, dies ohne Webinterface zu kompilieren,[4] da das Webinterface nur sehr lückenhaft entwickelt ist und praktisch keinen Mehrwert mit sich bringt. Entsprechend muss auch kein Webserver auf dem Raspberry Pi installiert werden.

6.4. Nagios

Nagios ist eine weit verbreitete Lösung zum Monitoring, es ermöglicht zentral Informationen über Verfügbarkeiten, Resourcenausnutzung usw. zu sammeln, sodass die Administratoren einen einfachen Überblick über den Zustand der Systeme erhalten. Existiert ein vom NDPMon-System erreichbarer Nagios Monitoring Host, dann kann auch NDPMon in Nagios eingebunden werden. Dann werden die Warnungen auch

[2] http://ndpmon.sourceforge.net/index.php?n=Doc.Installation - Abgerufen am 20.01.2014
[3] http://changux.co/ndpmon-run-raspberry/ - Abgerufen am 20.01.2014
[4] Indem die Parameter –enable-webinterface und –with-webdir beim ./configure Aufruf nicht mit übergeben werden.

dort angezeigt und der Administrator kann sich laufend über den Zustand des Dienstes informieren. Dies führt zu einer besseren Integration der Überwachungssysteme in die Umgebung und kann den Administratoren die Arbeit erleichtern.

Die Firewalls und Router sollten zunächst so konfiguriert werden, dass das Nagios Host-System über Netzwerk sowohl ICMP Nachrichten an den NDPMon Host versenden kann und Antworten erhält, als auch TCP Verbindungen zu diesem möglich sind. Nachfolgend sollte beachtet werden, auf Basis welchen IP Protokolls die Kommunikation stattfinden soll. In einer Dual-Stack Umgebung ist sowohl die Kommunikation über IPv4 als auch über IPv6 möglich. Hier empfiehlt es sich in diesem Fall, da ohnehin ein IPv6 Netz gegeben ist, genau wie im reinen IPv6 Betrieb, jegliche Kommunikation zwischen Nagios Host und NDPMon Host über IPv6 abzuwickeln. IPv6 bringt hierbei den Vorteil mit sich, dass das zur Abfrage verwendete Netz selbst durch NDPMon überwacht wird.

Generell ist jedoch auch die Nutzung von IPv4 unproblematisch, da nachfolgend alle über einen ICMP Ping hinausgehenden Überprüfungen über einen SSL- bzw. SSH-Tunnel durchgeführt werden. Auf diese Weise authentifiziert sich der NDPMon Host gegenüber dem Nagios Host mittels eines RSA Schlüsselpaars. Ein Angreifer könnte also in diesem Fall nicht als Man-in-the-Middle den Verkehr mit dem Nagios Host angreifen und so False Negatives erzeugen.

Zuerst sollte erfasst werden, ob eine Konnektivität zwischen NDPMon Host und Nagios Host besteht. Dazu ist es ausreichend, wenn der Nagios Host den NDPMon Host mittels eines Pings kontaktieren kann. Dazu kann sowohl bei IPv4 als auch bei IPv6 das *check_fping*[5] Plugin verwendet werden. Mittels der Parameter `-4` oder `-6` kann festgelegt werden, ob IPv4 oder IPv6 für den Ping verwendet werden soll. Kann der NDPMon Host mittels Ping nicht erreicht werden, deutet dies schon auf ein Problem mit dem Netzwerk oder dem Host hin.

Alle folgenden Plugins müssen lokal auf dem NDPMon System ausgeführt werden, die Ergebnisse der Überprüfungen werden dann an den Nagios Host zurückgeliefert. Dazu kommt standardmäßig der Nagios Remote Plugin Executor (nrpe)[6] zum Einsatz. Jedoch bietet dieser nur eine schlechte Unterstützung für Verschlüsselung mittels SSL. Generell ist das Aufrufen aller nachfolgenden Plugins auch über NRPE mittels SSL möglich, dennoch soll hier ein alternativer Weg beschrieben werden.

[5] http://exchange.nagios.org/directory/Plugins/Network-Protocols/ICMP/check_fping/details - Abgerufen am 28.01.2014

[6] http://wiki.monitoring-portal.org/nagios/howtos/nrpe - Abgerufen am 28.01.2014

Auf den meisten Linux Servern wird ein SSH Server zur Fernwartung und Verwaltung eingesetzt. Ein solcher SSH Server kann auch dazu genutzt werden, um die Plugins mittels *check_by_ssh* auszuführen. Es sollte ein spezieller *nagios* Benutzer eingerichtet werden, der nur Zugang zu den Nagios Plugins besitzt. Dann wird ein RSA Schlüsselpaar für den Nagios Server erstellt und dessen öffentlicher Schlüssel in der *authorized_hosts* Datei des *nagios* Benutzters hinzugefügt, um dem Nagios Host den Zugang über diesen Benutzer zu ermöglichen. Das genaue Vorgehen dabei wird in den Anleitungen „How to use check_by_ssh plugin for monitoring nagios or icinga“[7] und „Icinga check by ssh Plugin“[8] erläutert. Nachfolgend wird davon ausgegangen, dass der Nagios Host so konfiguriert wurde, dass er die Plugins auf dem NDPMon Host aufruft.

Initial sollte überprüft werden, ob der NDPMon Prozess überhaupt läuft. Dazu kann das standardmäßig im Nagios Plugin Paket enthaltene Plugin *check_procs*[9] verwendet werden. Es sollte damit überprüft werden, dass mindestens ein *ndpmon* Prozess läuft, andernfalls ist eine Warnung bzw. Fehler auszugeben.

Danach sollten die letzten Warnungen des NDPMon untersucht werden. Dazu muss zuerst die Konfigurationsdatei *config_ndpmon.xml* so ergänzt werden, dass bei Alerts mit hoher bzw. niedriger Priorität das Script *alerts_to_xml.py* aufgerufen wird. Dieses speichert die gemeldeten Ereignisse dann in der Datei *alerts.xml* . Mittels des eigens entwickelten Nagios Plugins *check_ndpmon_alerts.py*[10] kann dieses Ergeignislog dann untersucht werden. Dabei kann mittels der Parameter *-H <timeout>* und *-L <timeout>* ein Timeout für Alerts mit hoher bzw. niedriger Priorität eingerichtet werden. Als erstes Argument wird dem Plugin der Pfad zur Datei *alerts.xml* des NDPMon übergeben. Wird das Plugin aufgerufen, erfolgt nur eine kritische Rückmeldung, wenn ein Alert mit hoher Priorität vorliegt, der noch nicht die Timeout-Zeit H überschreitet. Eine Warnung wird zurückgegeben, wenn in der Timeout-Zeit L ein Alert niedriger Priorität existiert. Dementsprechend sollten die Timeouts nicht zu kurz gewählt werden, sodass ein Angriff auch noch einige Zeit im Webinterface sichtbar ist.

Letztlich sollten noch die Resourcen des NDPMon Systems überwacht werden, die

[7] http://linuxdrops.com/how-to-use-check_by_ssh-plugin-for-monitoring-nagios-or-icinga/ - Abgerufen am 28.01.2014

[8] http://www.thomas-krenn.com/de/wiki/Icinga_check_by_ssh_Plugin - Abgerufen am 28.01.2014

[9] http://wiki.monitoring-portal.org/nagios/plugins/check_procs - Abgerufen am 28.01.2014

[10] *Quellcode siehe Listing A.1*

drei wesentlichen Faktoren um zu überprüfen wie ausgelastet das System ist, sind verwendeter RAM, CPU Auslastung und Füllstand der Festplatte. Dafür seien folgende Plugins empfohlen:

CPU Auslastung check_cpu_performance[11]

RAM Verwendung check_mem.sh[12]

Festplattenfüllstand check_disk[13]

Zusätzlich kann der Administrator noch beliebige weitere Nagios Plugins einrichten um beispielsweise die CPU Temperatur zu überwachen oder ähnliches.

6.5. Einsatz

Im praktischen Einsatzszenario würden Administratoren einen Raspberry Pi mit Raspbian und der entsprechenden NDPMon Version einrichten wie jedes normale Linux Serversystem. Dabei sollte SSH auf Public Key Authentifizierung mit dem Schlüssel der Administratoren beschränkt werden. Wird der private Schlüssel sicher aufbewahrt, so kann so sichergestellt werden, dass kein Angreifer das System über schlechte Passwörter übernimmt.

Danach kann das konfigurierte Überwachungssystem mit dem zu überwachenden Link verbunden werden. Dazu muss der Ethernet Port lediglich mit einem Switch Port, der zu dem Link gehört verbunden werden. Die Entwickler von NDPMon empfehlen dem System aus Gründen der Stabilität statisch eine globale IPv6 Adresse zuzuweisen. Eine Nutzung von SLAAC ist jedoch grundsätzlich auch möglich. Nach der Zuweisung einer IPv6 Adresse sollte auf dem Netzwerkinterface der NDP Multicast-Verkehr empfangen werden können.

Mittels *ndpmon -c* kann der Lernprozess angestoßen werden. NDPMon wird dann aus dem eintreffenden Neighbor Discovery Verkehr eine Konfiguration für den Link erstellen. Nach einiger Zeit, abhängig von Verkehrsaufkommen und der Größe des Netzes, kann der Lernvorgang beendet werden. Anschließend sollte der Administrator die Konfiguration kontrollieren und eigene Anpassungen durchführen. So soll

[11] http://exchange.nagios.org/directory/Plugins/System-Metrics/CPU-Usage-and-Load/Check-CPU-Performance/details - Abgerufen am 30.01.2014

[12] http://exchange.nagios.org/directory/Plugins/System-Metrics/Memory/check_mem-2Esh/details - Abgerufen am 30.01.2014

[13] https://nagios-plugins.org/doc/man/check_disk.html - Abgerufen am 30.01.2014

sichergestellt werden, dass Fehler bei der automatischen Lernfunktion erkannt und behoen werden.

Um die korrekte Funktion des NDPMon zu testen, sollte der NDPMon-Daemon anschließend vorerst ohne aktivierte Gegenmaßnahmen eingesetzt werden. Die Administratoren erhalten bei Alerts nur Benachrichtigungen, z.B. in Form von E-Mails. Es werden zunächst keine Gegenmaßnahmen durchgeführt, die Auswirkungen auf die Funktionsfähigkeit des Links haben können.

Um einen aktiven Schutz vor Angriffen umzusetzen, können nach der Lernphare und einer Testphase von einigen Tagen bis Wochen die Gegenmaßnahmen aktiviert werden.

Abbildung 6.1.: Raspberry Pi mit NDPMon im Einsatz

6.6. Vorteile

Der Raspberry Pi bietet eine kostengünstige Plattform zur Integration des NDPMon in das Netz. Durch seinen geringen Anschaffungspreis und Stromverbrauch entstehen nur vergleichsweise niedrige Mehrkosten. Dennoch kann ein hohen Sicherheitsgewinn durch den Einsatz von NDPMon erreicht werden.

Auch das Aufstellen des Raspberry Pi gestaltet sich einfach, denn durch seine kleine Größe wird keine 19“ Höheneinheit benötigt. Der Raspberry Pi kann wegen seiner kleinen Maße an der Rackschiene auf der Rückseite des Schranks befestigt werden. So wird nicht kostbarer Platz im Serverschrank belegt. Auch wenn der Serverschrank keinen freien Platz für weitere Server besitzt, so lässt sich der Raspberry Pi in der Regel trotzdem unterbringen.

Da die Hardware über keine mechanischen Komponenten wie Festplatten oder Lüfter verfügt, ist der Wartungsaufwand insbesondere für die Befreiung von Staub sehr gering.

Gleichzeitig handelt es sich bei dem Raspberry Pi um eine Standardplattform, die weit verbreitet und über verschiedenste Distributoren verfügbar ist. Durch die identische Hardwarekonfiguration aller Überwachungssysteme wird die Konfiguration und Wartung erleichtet. Durch die gute Unterstützung automatischer Updates durch Debian kann sichergestellt werden, dass sicherheitskritische Updates zeitnah eingespielt werden.

Wegen der geringen Kosten ist es möglich für jeden Link ein eigenes NDPMon Überwachungssystem zu verwenden. So kann verhindert werden, dass ein System mit mehreren Links verbunden ist und so ein attraktives Ziel für Angreifer bietet, die in andere Teile des Unternehmensnetzes vordringen wollen.

6.7. Nachteile

Als Nachteil des Raspberry Pi ist zu nennen, dass es sich um ein recht leistungsschwaches System handelt. Werden sehr große Links verwendet, die viel Multicast-Verkehr erzeugen, so kann es unter Umständen zu Performance-Engpässen kommen. Dabei ist jedoch anzumerken, dass die Performance in Netzen in denen soviel Multicast-Verkehr auftritt ohnehin stark beeinträchtigt sein kann. Es sollte somit angestrebt werden die Links nicht zu groß werden zu lassen. Bei Tests in kleinen Netzen stellte die relativ geringe Leistungsfähigkeit des Raspberry Pi kein Problem dar.

Da sich NDPMon, wie in Abschnitt 6.4 beschrieben, sehr gut mit Nagios kombinieren lässt, kann im gleichen Zuge auch die Systemauslastung der Überwachungssysteme überwacht werden. Auf diese Weise kann erkannt werden, wenn der Raspberry Pi überlastet ist. Als Reaktion auf eine solche Überlastung kann entweder der Link

restrukturiert oder ein leistungsstärkeres System für NDPMon eingesetzt werden. Dies lässt eine Optimierung des mit dem Einsatz von NDPMon verbundenen Resourcenaufwands zu.

Auch wenn der Raspberry Pi mit relativ geringem Wartungsaufwand auskommt, müssen dennoch alle Überwachungssysteme jeweils auf dem aktuellsten Stand gehalten werden. Dies kann, abhängig von der Anzahl der Links auf denen NDPMon eingesetzt wird, relativ aufwendig sein.

Da der Raspberry Pi nur passiv gekühlt wird und über keine Lüfter verfügt, ist zu überprüfen ob Überhitzung in dem Serverschrank ein Problem darstellt. Dies ist jeweils abhängig von der Umgebung in der das System eingesetzt wird. Vor der Einführung sollte eine Überprüfung der Eignung des Raspberry Pi mit Blick auf das Kühl- und Lüftungskonzept durchgeführt werden. Andernfalls könnte es zu Ausfällen der Hardware kommen, während derer das Netz ungeschützt ist.

6.8. Bewertung

Der Raspberry Pi eignet sich gut als Plattform für NDPMon. Es handelt sich somit um eine kostengünstige Möglichkeit zur Integration einer reaktive Schutzmaßnahme in die Netze. Für Links normaler Größe reicht die Leistungsfähigkeit aus. Durch sein kompaktes Format lässt sich der Raspberry Pi einfach installieren.

Die Einführung von NDPMon kann durch eine einheitliche Lösung, basierend auf dem Raspberry Pi, beschleunigt und für Administratoren stark vereinfacht werden.

7. Fazit

Es existieren verschiedene Angriffe auf lokale IPv6 Netzwerke, die eine schwerwiegende Beeinträchtigungen der Schutzziele (siehe Abschnitt 2.2) zur Folge haben können.

Je nach Sicherheitsanforderungen ist bei der Betrachtung der Netzwerksicherheit auch das Risiko interner Angreifer und lokaler Angriffe auf Netzwerke zu berücksichtigen. Deshalb sind Gegenmaßnahmen zur Abwehr derartiger Bedrohungen notwendig.

Bei näherer Betrachtung der verfügbaren Maßnahmen wird jedoch schnell klar, dass diese oftmals wenig durchdacht sind. Einerseits sind ihre Implementierungen wie beispielsweise bei RA-Guard noch lückenhaft, da sie sich durch Protokollbesonderheiten von IPv6 umgehen lassen. Andererseits existieren wie bei SEcure Neighbor Discovery bereits konzeptionelle Probleme, die die Maßnahme für den großflächigen Einsatz untauglich machen.

Außerdem erfordern viele Maßnahmen einen hohen finanziellen Aufwand, wenn sie in bestehende Netze integriert werden sollen. Es müssen beispielsweise Teile der Netzwerkhardware ausgetauscht werden, sodass diese über die notwendigen Funktionen verfügen.

Reaktive Maßnahmen (wie NDPMon) sind aktuell am besten für den praktischen Einsatz geeignet. Mit ihnen kann die Sicherheit gegenüber den meisten Angriffen stark verbessert werden, ohne einen tiefen Eingriff in die Netzwerkinfrastruktur vornehmen zu müssen. Wie in Kapitel 6 beschrieben, lässt sich NDPMon mittels einer Plattform wie dem Raspberry Pi, mit vergleichsweise geringem Aufwand in die meisten Netze integrieren.

Die saubere Strukturierung der verschiedenen Netze (siehe Abschnitt 4.4), nach Kriterien wie Klassifizierung, Typ und Organisationseinheit kann die Auswirkungen eines erfolgreichen Angriffs minimieren. Auch wenn eine derartige Restrukturierung mit hohem Aufwand verbunden sein kann, so ergänzt sie dennoch gut die übrigen Maßnahmen und ist auch Sicht der Netzplanung ebenfalls zu empfehlen.

Da die Verbreitung des IPv6-Protokolls erst in den letzten Jahren einem starken Wachstum unterliegt, gewinnt jetzt auch die Sicherheit derartiger Netze zunehmend an Bedeutung. In den letzten Monaten flossen noch zahlreiche Änderungen im Bezug auf das Neighbor Discovery Protocol in die entsprechenden RFCs ein, deren Ziel es war die Absicherung von IPv6 zu erleichtern.

Diese tiefgreifenden Änderungen stellen wiederum die Hersteller von Netzwerkhardware und die Entwickler von IPv6 Protokollstacks vor Herausforderungen. Sie müssen die Änderungen in die Protokollimplementierungen aller betroffenen Geräte übernehmen und entsprechende Updates bereitstellen. Vorraussichtlich wird es noch einige Jahre dauern, bis ein Großteil der Produkte diese Änderungen berücksichtigt.

Es ist zumindest langfristig damit zu rechnen, dass immer mehr der eingesetzten Switches über Schutzmaßnahmen wie RA-Guard und FCFS-SAVI verfügen. Durch die Änderungen der RFCs zur Neighbor Discovery ([RFC7112], [RFC6980]) werden diese Maßnahmen zukünftig effektiv vor den meisten Angriffen schützen können.

Vorerst ist es aber in den wenigsten Fällen sinnvoll die aktuelle Hardware direkt auszutauschen, da es vielen Implementierungen noch an der Reife für den produktiven Einsatz mangelt. Entsprechende Funktionen sollten aber bei zukünftigen Beschaffungsentscheidungen berücksichtigt werden, da Schutzmaßnahmen auf Ebene der Netzwerkhardware in einigen Jahren vorraussichtlich so selbstverständlich sein werden, wie heute der Schutz vor ARP-Spoofing beispielsweise mittels Dynamic ARP Inspection.[1]

Wegen ihrer zahlreichen Nachteile sind kryptografische Schutzmaßnahmen sind zur Absicherung von IPv6 aktuell noch nicht einsetzbar. Es bleibt jedoch offen, ob alternative Lösungsansätze zukünftig eine kryptografische Absicherung von NDP erlauben.

Als Ansatz zur Absicherung der Neighbor Discovery lassen sich möglicherweise *proof-of-work*-Protokolle für den Versand von Neighbor Advertisements einsetzen. Bei ihnen muss der Absender eine aufwendige kryptografische Berechnung durchführen, während die Überprüfung des Ergebnisses durch den Empfänger sehr wenig Aufwand erfordert. Eines der bekanntesten solchen Protokolle ist Hashcash[2], welches unter anderem auch bei Bitcoin zum Einsatz kommt.

[1] http://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=8 - Abruf am 20.02.2014
[2] http://www.hashcash.org/ - Abruf am 20.02.2014

Solche Protokolle könnten, zusammen mit Verfahren der identitätsbasierten Kryptografie, eine Möglichkeit zur Unterbindung der geschilderten Angriffe durch gefälschte Neighbor Advertisements bieten.

Derartige Ansätze und inwiefern sich auf ähnliche Weise auch die Router Discovery absichern ließe sind jedoch noch nicht weiter analysiert worden. Hier besteht zukünftig noch die Möglichkeit weiterer Untersuchungen zur Absicherung von IPv6 im LAN.

Literaturverzeichnis

[RFC3971] Arkko, J. ; Kempf, J. ; Zill, B. ; Nikander, P.: *SEcure Neighbor Discovery (SEND).* RFC 3971 (Proposed Standard). http://www.ietf.org/rfc/rfc3971.txt. Version: März 2005 (Request for Comments). – Updated by RFCs 6494, 6495, 6980

[RFC3972] Aura, T.: *Cryptographically Generated Addresses (CGA).* RFC 3972 (Proposed Standard). http://www.ietf.org/rfc/rfc3972.txt. Version: März 2005 (Request for Comments). – Updated by RFCs 4581, 4982

[SENDSavi] Bagnulo, M. ; Garcia-Martinez, A.: *SEND-based Source-Address Validation Implementation.* http://tools.ietf.org/html/draft-ietf-savi-send-06. Version: 04.10.2013

[ISecFund04] Blackley, J.A. ; Peltier, T.R. ; Peltier, J.: *Information Security Fundamentals.* Taylor & Francis, 2004. – ISBN 9780203488652

[Boek2012] Bök, Patrick-Benjamin ; Tüchelmann, York: *Planung und Auslegung von Computernetzen - Systematik und methodische Vorgehensweise.* 1. Aufl. Bochum : W3L-Verlag, 2012. – ISBN 978–3–868–34017–4

[CVE-2011-2395] *CVE-2011-2395.* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2395. Version: 12.12.2011

[RFC2460] Deering, S. ; Hinden, R.: *Internet Protocol, Version 6 (IPv6) Specification.* RFC 2460 (Draft Standard). http://www.ietf.org/rfc/rfc2460.txt. Version: Dezember 1998 (Request for Comments). – Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112

[GONTND13] Gont, F. ; Bonica, R. ; Liu, W.: *Security Assessment of Neighbor Discovery (ND) for IPv6.* http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-02. Version: 18.11.2013

[RFC5424] Gerhards, R.: *The Syslog Protocol*. RFC 5424 (Proposed Standard). http://www.ietf.org/rfc/rfc5424.txt. Version: März 2009 (Request for Comments)

[RFC7112] Gont, F. ; Manral, V. ; Bonica, R.: *Implications of Oversized IPv6 Header Chains*. RFC 7112 (Proposed Standard). http://www.ietf.org/rfc/rfc7112.txt. Version: Januar 2014 (Request for Comments)

[RFC6980] Gont, F.: *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*. RFC 6980 (Proposed Standard). http://www.ietf.org/rfc/rfc6980.txt. Version: August 2013 (Request for Comments)

[RFC7113] Gont, F.: *Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)*. RFC 7113 (Informational). http://tools.ietf.org/html/rfc7113. Version: Februar 2014

[IPv6HAGEN09] Hagen, S.: *IPv6: Grundlagen - Funktionalität - Integration*. Sunny Connection AG, 2009. – ISBN 9783952294222

[HDYv6WP] Hamdy, Safuat: *IPv6 - Die grundlegenden Funktionen, Bedrohungen und Maßnahmen*. Secorvo White Paper, WP18. Version: Oktober 2013. http://www.secorvo.de/publikationen/secorvo-wp18.pdf

[CiscoIPv6Sec] Hogg, Scott ; Vyncke, Eric: *IPv6 Security*. Cisco Press Networking Technology, 2008

[ITUX200] ITU: *ITU-T Rec. X.200 (1994 E)*. http://www.itu.int/rec/T-REC-X.200-199407-I. Version: Juli 1994. – Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model

[RFC6106] Jeong, J. ; Park, S. ; Beloeil, L. ; Madanapalli, S.: *IPv6 Router Advertisement Options for DNS Configuration*. RFC 6106 (Proposed Standard). http://www.ietf.org/rfc/rfc6106.txt. Version: November 2010 (Request for Comments)

[RFC6105] Levy-Abegnoli, E. ; Velde, G. V. ; Popoviciu, C. ; Mohacsi, J.: *IPv6 Router Advertisement Guard*. RFC 6105 (Informational). http://www.ietf.org/rfc/rfc6105.txt. Version: Februar 2011 (Request for Comments)

[RFC6620] Nordmark, E. ; Bagnulo, M. ; Levy-Abegnoli, E.: *FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses*. RFC 6620 (Proposed Standard). http:

//www.ietf.org/rfc/rfc6620.txt. Version: Mai 2012 (Request for Comments)

[RFC3756] Nikander, P. ; Kempf, J. ; Nordmark, E.: *IPv6 Neighbor Discovery (ND) Trust Models and Threats*. RFC 3756 (Informational). http://www.ietf.org/rfc/rfc3756.txt. Version: Mai 2004 (Request for Comments)

[RFC4861] Narten, T. ; Nordmark, E. ; Simpson, W. ; Soliman, H.: *Neighbor Discovery for IP version 6 (IPv6)*. RFC 4861 (Draft Standard). http://www.ietf.org/rfc/rfc4861.txt. Version: September 2007 (Request for Comments). – Updated by RFCs 5942, 6980, 7048

[RFC826] Plummer, D.: *Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. RFC 826 (INTERNET STANDARD). http://www.ietf.org/rfc/rfc826.txt. Version: November 1982 (Request for Comments). – Updated by RFCs 5227, 5494

[Schaefer2003] Schäfer, Günter: *Netzsicherheit - algorithmische Grundlagen und Protokolle*. 1. Aufl. Köln : Dpunkt-Verlag, 2003. – ISBN 978–3–898–64212–5

Glossar

ARP	Das Address Resolution Protocol ist ein Protokoll zur Ermittlung der zu einer IPv4 Adresse gehörenden MAC Adresse.
DAD	siehe Duplicate Address Detection
Dual-Stack Betrieb	Gleichzeitiger Betrieb von IPv4 und IPv6 in einem Netzwerk.
Duplicate Address Detection	siehe Abschnitt 3.4
False Negative	Beschreibt die Situation, in der ein positives Ereignis vorliegt, dieses jedoch nicht erkannt wird.
False Positive	Beschreibt die Situation, in der ein Ereignis gemeldet wird, dieses jedoch nicht vorliegt.
Host	Ist ein System, welches ins Netzwerk eingebunden ist und für dieses Dienste bereitstellt.
Interface	Netzwerkschnittstelle eines Nodes
Internetprotokoll	Die Vermittlungsschicht zur Kommunikation zwischen Systemen im Internet.
IP-Header	Teil der IP Datenpakete, der protokollspezifische Informationen enhält.
IPv4	Das Internetprotokoll in der Version 4.
IPv6	Das Internetprotokoll in der Version 6.
IPv6 Header Chain	Der IPv6 Header, alle Extension Header und der Header des Upper Layer Protocol (ULP).

LAN	Ein LAN (Local Area Network) beschreibt ein lokales Rechnernetz.
Link	Beschreibt die Gesamtheit aller Systeme welche ohne Routing miteinander kommunizieren können.
Monitoring	Systematische Erfassung und Beobachtung von Prozessen sowie Vorgängen
Multicast	Nachrichtenübermittlung von einem Punkt an eine Gruppe von Empfängern
NA	siehe Neighbor Advertisement
NDP	siehe Neighbor Discovery Protocol
Neighbor	Node der sich on-link befindet.
Neighbor Advertisement	siehe Abschnitt 3.1
Neighbor Cache	Zwischenspeicher für die Assoziationen zwischen IPv6 und MAC Adresse
Neighbor Discovery Protocol	Protokoll auf Basis von ICMPv6, unter anderem zur Auflösung von IPv6 in Link-Layer-Adressen und Router Discovery.
Neighbor Solicitation	siehe Abschnitt 3.1
Neighbor Unreachability Detection	siehe Abschnitt 3.2
Node	Ein System welches über mindestens ein Netzwerkinterface mit einem Netzwerk verbunden ist.
NS	siehe Neighbor Solicitation
NUD	siehe Neighbor Unreachability Detection
off-link	Bezeichnung für Nodes, die nur mittels Routing erreicht werden können.

on-link	Bezeichnung für Nodes, die ohne Routing erreicht werden können.
Payload	Nutzlast eines Protokolls, also nicht Header des entsprechenden Protokolls. Enthält in der Regel die ULPs.
Performance	Leistungsfähigkeit, hier eines Netzwerks, bestehend aus Antwortzeiten, zur Verfügung stehender Bandbreite und Zuverlässigkeit des Netzes.
Präfix	Höchstwertige Teil eine IPv6 Adresse, der einen zugeordneten Netzbereich beschreibt.
RA	siehe Router Advertisement
Router Advertisement	siehe Abschnitt 3.3
Router Solicitation	siehe Abschnitt 3.3
RS	siehe Router Solicitation
SLAAC	Stateless Address Autoconfiguration erlaubt die automatische zustandslose Konfiguration der IPv6 Adresse eines Nodes
Uplink	Internetzugangsleitung, also Verbindung in das restliche Internet. In der Regel mittels eines ISPs
ULP	siehe Upper Layer Protocols
Upper Layer Protocols	Sind die höheren Protokollschichten, im Fall von IP in der Regel ICMP, TCP und UDP.

A. NDPMon Nagios Integration

A.1. check_ndpmon_alerts.py

```
#!/usr/bin/env python

import logging
import os
import time
import datetime
from optparse import OptionParser
import xml.dom, xml.dom.minidom

logging.basicConfig(level=logging.DEBUG, format='%(asctime)s - %(
    message)s', datefmt='%Y-%m-%d %I:%M:%S')

# Exit statuses recognized by Nagios
UNKNOWN = -1
OK = 0
WARNING = 1
CRITICAL = 2

## NDPMon the alert reasons as set in the arrays below, define when a
    alert is considered as CRITICAL or as a WARNING for Nagios

# alert reasons that are handled as CRITICAL
HIGH_PRIORITY_ALERTS = [
"wrong router redirect ip",
"wrong router redirect mac",
"wrong router redirect",
"wrong couple IP/MAC in RD",
"wrong router ip",
"wrong router mac",
"wrong ipv6 router",
"wrong RA flags",
"wrong RA params",
"wrong prefix",
"wrong RA prefix option lifetimes",
"RA prefix option valid lifetime too short",
"wrong RA prefix option params",
```

```
"wrong RA mtu option",
"wrong RA RDNSS option",
"wrong RA DNSSL option",
"wrong RA Route Info option",
"spoofed addresses",
"user defined rule matched",
"NA router flag",
"dad dos"
]

# alert reasons that are handled as WARNING
LOW_PRIORITY_ALERTS = [
"NA LLA mismatch",
"ethernet mismatch",
"bogon",
"unknown mac vendor",
"changed ethernet address",
"wrong couple MAC/LLA",
"flip flop",
"wrong couple IP/MAC"
]

# other possible reasons used by NDPMon
# OTHER_ALERTS = [
# "NA multicast target",
# "NA Override flag",
# "ethernet broadcast",
# "ip multicast",
# "wrong ipv6 hop limit",
# "new station",
# "new lla",
# "new IP",
# "reused old ethernet address",
# "new activity"
# ]

# create alert dict from xml key-value pairs
def parseAlert(values):
  if not "vendor" in values.keys():
    values["vendor"] = ""
  alert = {
      "time"   : datetime.datetime.fromtimestamp(float(values["time_sec
          "])),
      "reason": values["reason"].strip(),
      "mac"    : values["mac"],
      "vendor": values["vendor"],
      "ipv6"   : values["ipv6"]
  }
  return alert
```

```
# convert an alert dict to a string
def alertToString(alert):
  res = []
  for k,v in alert.iteritems():
    res.append("%s\t\t:\t%s" % (k,v))
  return '\n'.join(res)

# validate if the alert is CRITICAL or a WARNING
def checkAlert(alert, high_timeout, low_timeout):
  high_ts = datetime.datetime.now() - datetime.timedelta(seconds=
      high_timeout)
  low_ts = datetime.datetime.now() - datetime.timedelta(seconds=
      low_timeout)
  if high_ts < alert["time"] and alert["reason"] in
      HIGH_PRIORITY_ALERTS:
    logging.critical("Found critical alert!\n%s" % (alertToString(alert
        ),))
    return CRITICAL
  if low_ts < alert["time"] and alert["reason"] in LOW_PRIORITY_ALERTS:
    logging.critical("Found warning alert!\n%s" % (alertToString(alert)
        ,))
    return WARNING
  return OK


if __name__ == "__main__":
  # parse arguments
  parser = OptionParser()
  parser.add_option('-H', '--high-priority-timeout', dest='high_prio',
      default=6000, type="int")
  parser.add_option('-L', '--low-priority-timeout', dest='low_prio',
      default=1000, type="int")
  parser.add_option('-v', '--verbose', dest='verbose', action='
      store_true', default=False)
  parser.add_option('-q', '--quiet', dest='verbose', action='
      store_false')
  options, args = parser.parse_args()

  if len(args) < 1:
    logging.critical("First argument MUST be the path to the alerts.xml
        file!")
    raise SystemExit, CRITICAL

  # parse XML file
  try:
    doc = xml.dom.minidom.parse(args[0])
  except Exception as e:
```

```
    logging.critical("Could not parse given XML file: %s" % str(args
        [0]))
    logging.exception(e)
    raise SystemExit, CRITICAL

  # extract alert nodes
  alert_nodes = doc.getElementsByTagName('alert')
  alerts = []
  for alert_node in alert_nodes:
    try:
      children = [x for x in alert_node.childNodes if x.nodeType ==
          alert_node.ELEMENT_NODE]
      val_children = {}
      for c in children:
        val_children[c.tagName] = ''.join([x.nodeValue for x in c.
            childNodes])
      alerts.append(parseAlert(val_children))
    except Exception as e:
      logging.warning("Error in XML alert format!")
      logging.exception(e)

  # check if there is a relevant update
  results = []
  for alert in alerts:
    results.append(checkAlert(alert, options.high_prio, options.
        low_prio))

  # set the returncode according to the results
  if CRITICAL in results:
    raise SystemExit, CRITICAL
  elif WARNING in results:
    raise SystemExit, WARNING
  else: # no alerts found
    logging.info("No alerts found!")
    raise SystemExit, OK
```

A.2. alerts.xml

Beispielausgabe des NDPMon für Testzwecke

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="alerts.xsl"?>
<alerts>
  <alert>
    <time>Tue Feb  4 22:15:42 2014</time>
    <time_sec>1391548542.473047</time_sec>
    <reason>wrong couple IP/MAC</reason>
```

```
    <mac>3c:97:0e:46:6a:c1</mac>
    <vendor>Lenovo</vendor>
    <ipv6>fe80::6267:20ff:fec5:6db8</ipv6>
  </alert>
</alerts>
```